INSANITY IS - OR HOW CAN WE FINALLY MAKE PROGRESS ON SECURING OUR COMPUTING INFRASTRUCTURE?

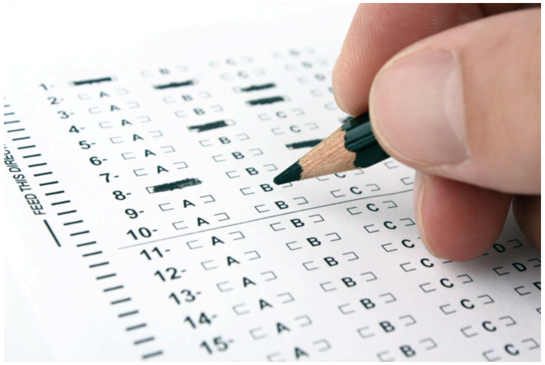
Henning Schulzrinne
Columbia University

March 2015

Overview

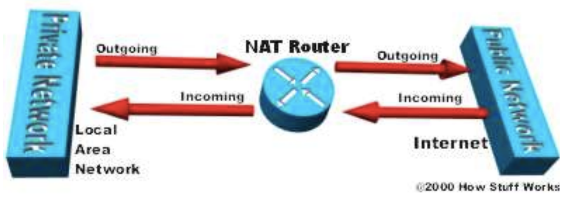
- Security fallacies
  - Stop blaming (and "educating") users
  - Reduce the value of targets
  - Avoid "small mistake, huge cost"
  - Secure key identifiers
  - Make it hard to scale attacks
  - Make it easy to detect loss
  - Design fraud-resistant systems
  - Worry about DOS attacks on humans
- Robo-calling and caller ID spoofing
- Professional responsibility to not just patch things

Pattern of failure



Pattern of failure

→



ICE
STUN
TURN

~~secure OS & applications~~

→

MS-ISAC MULTI-STATE
Information Sharing & Analysis Center

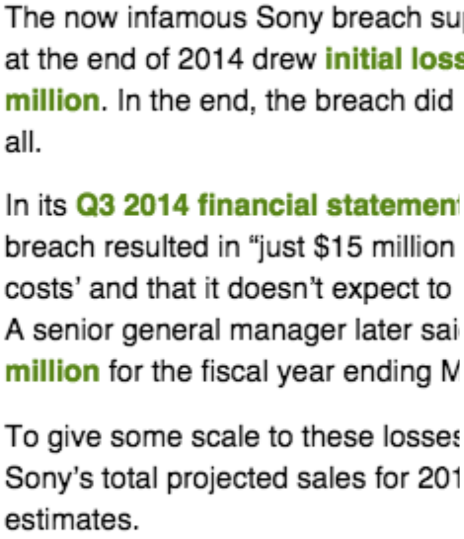
Be careful with e-mail

What are you worried about?

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Goal	click fraud, DDOS	empty bank account	
What doesn’t help	Encrypt all protocols	firewall	Updates (zero-days)
What might	Update software; firewall	Defense in depth	Encrypt all protocols

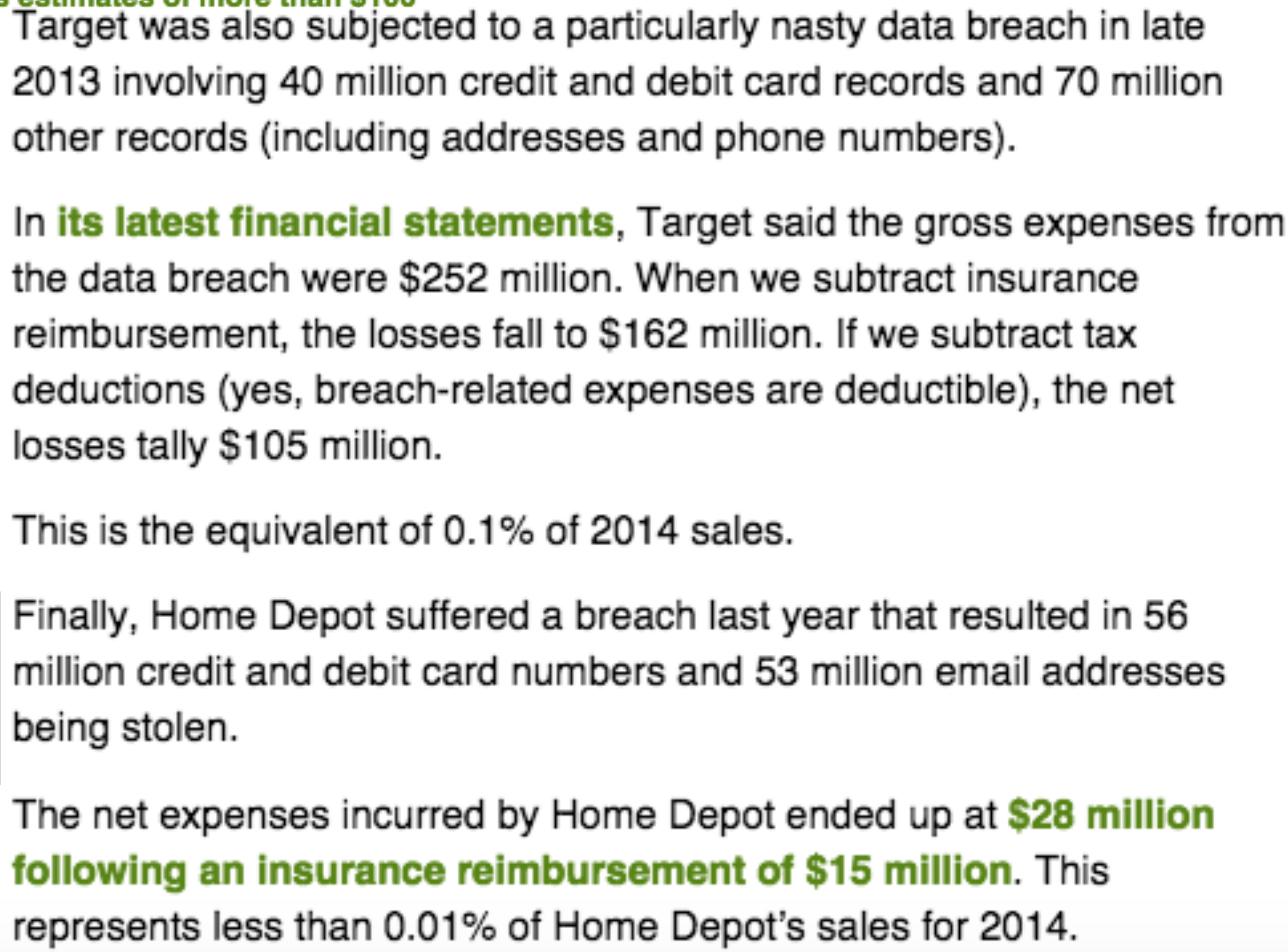
Limited incentive for companies



The now infamous Sony breach supposedly perpetrated by North Korea at the end of 2014 drew **initial loss estimates of more than $100 million**. In the end, the breach did all.

In its **Q3 2014 financial statemen** breach resulted in "just $15 million costs' and that it doesn't expect to A senior general manager later sai **million** for the fiscal year ending M

To give some scale to these losse Sony's total projected sales for 201 estimates.



Target was also subjected to a particularly nasty data breach in late 2013 involving 40 million credit and debit card records and 70 million other records (including addresses and phone numbers).

In **its latest financial statements**, Target said the gross expenses from the data breach were $252 million. When we subtract insurance reimbursement, the losses fall to $162 million. If we subtract tax deductions (yes, breach-related expenses are deductible), the net losses tally $105 million.

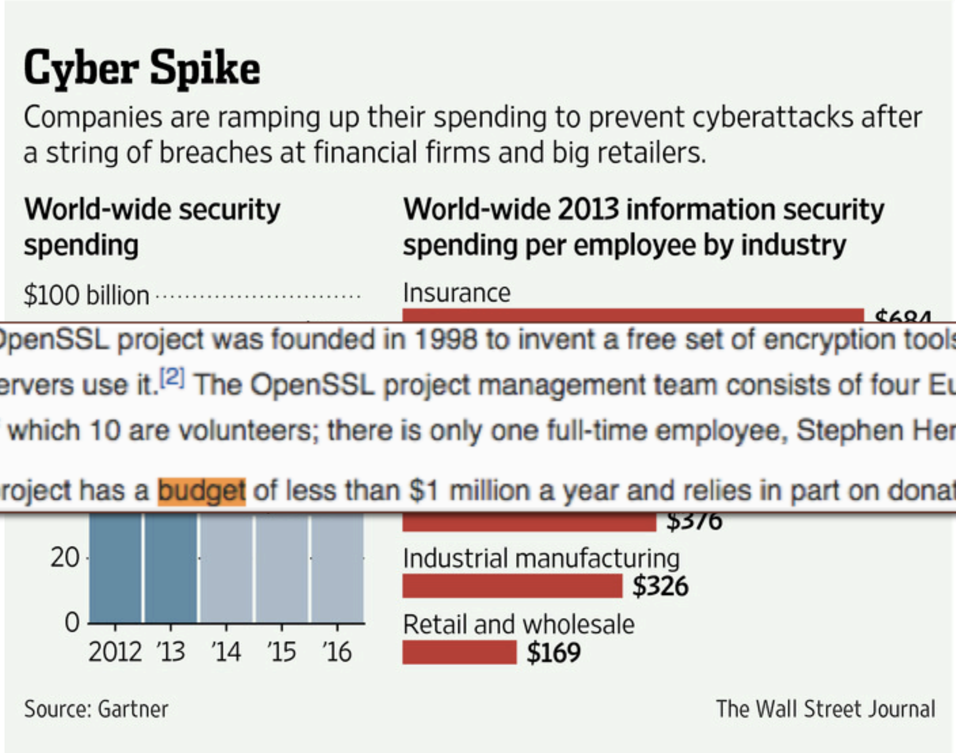
This is the equivalent of 0.1% of 2014 sales.

Finally, Home Depot suffered a breach last year that resulted in 56 million credit and debit card numbers and 53 million email addresses being stolen.

The net expenses incurred by Home Depot ended up at **$28 million following an insurance reimbursement of $15 million**. This represents less than 0.01% of Home Depot's sales for 2014.

doesn't account
for costs to customers
and credit card companies

Tragedy of the Commons, again



Source: Gartner

The Wall Street Journal

The OpenSSL project was founded in 1998 to invent a free set of encryption tools for the code used on the Internet. As of 2014 two thirds of all webservers use it.[2] The OpenSSL project management team consists of four Europeans. The entire development group consists of 11 members, out of which 10 are volunteers; there is only one full-time employee, Stephen Henson, the lead developer.[3]

The project has a budget of less than $1 million a year and relies in part on donations. Steve Marquess, a former military consultant in Maryland

Six dumbest ideas in security (Ranum 2005)

- Default permit
  - firewall rules
  - code execution
- Enumerating badness
  - track goodness instead
- Penetrate and patch
  - Java, Adobe Flash
  - ←→ Qmail, PostFix compartmentalization
- Hacking is cool
  - → good engineering is cool
- Educating users
- Action is better than inaction

Six other dumb ideas

1. (US) credit cards
2. Social security numbers – public key cryptography, redefined
3. Checks
4. Linux ssh security defaults
   - allow root login; no 2-factor built-in; no automated context login
5. Allowing user applications to write any file
   - → ransomware
6. No type checking for external input data for web languages
   - we won't even talk about PHP `register_globals`

Security approach: blame the victim

Run 10 anti-virus systems!

Choose passwords you can't remember!

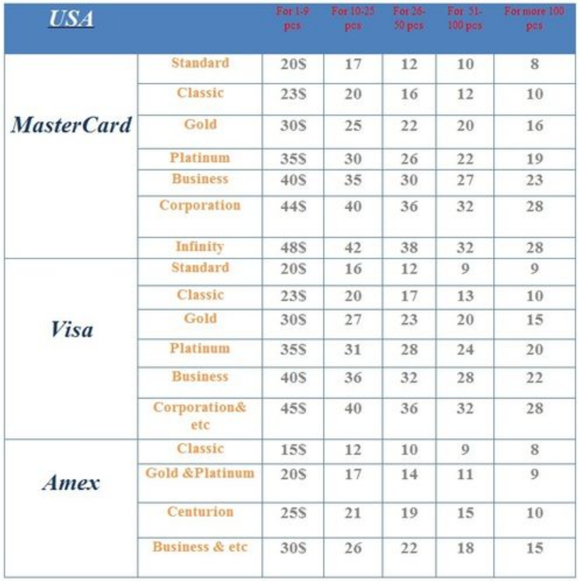
Pay cash!

Don't click on that link!

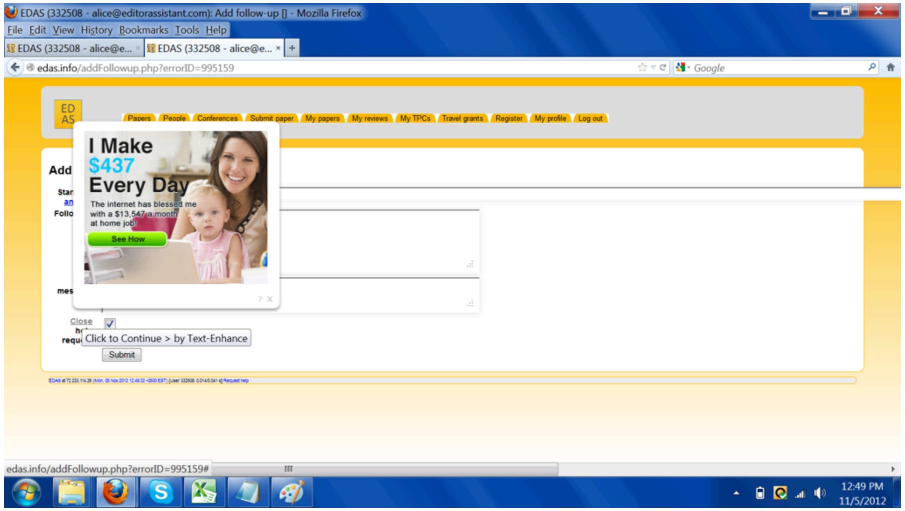
Choose another operating system!

Nobody cares about you!

- Unless you have access to high-value information
  - sometimes for individualized identity theft
- You are only valuable as
  - a credit card number that can be resold in bulk ($2-$8)
  - a machine usable for …
    - DOS attacks
    - email spam
      - 88% of spam sent by botnet
    - a machine usable for advertising click fraud
      - watch highlighted links!
      - $0.002-0.003/click → $0.50-$2 CPM



USA		For 1-9 pcs	For 10-25 pcs	For 26-50 pcs	For 51-100 pcs	For more 100 pcs
MasterCard	Standard	20$	17	12	10	8
	Classic	23$	20	16	12	10
	Gold	30$	25	22	20	16
	Platinum	35$	30	26	22	19
	Business	40$	35	30	27	23
	Corporation	44$	40	36	32	28
	Infinity	48$	42	38	32	28
Visa	Standard	20$	16	12	9	9
	Classic	23$	20	17	13	10
	Gold	30$	27	23	20	15
	Platinum	35$	31	28	24	20
	Business	40$	36	32	28	22
	Corporation& etc	45$	40	36	32	28
Amex	Classic	15$	12	10	9	8
	Gold &Platinum	20$	17	14	11	9
	Centurion	25$	21	19	15	10
	Business & etc	30$	26	22	18	15



EDAS (332508 - alice@editorassistant.com): Add follow-up [] - Mozilla Firefox

edas.info/addFollowup.php?errorID=995159

I Make $437 Every Day

The internet has blessed me with a $13,547 a month at home job!

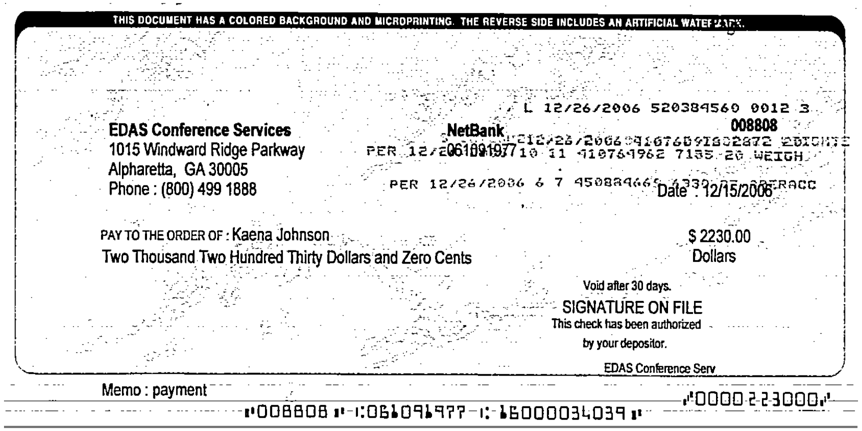
Click to Continue > by Text-Enhance

EDAS at 72.233.114.26 (Mon, 05 Nov 2012 12:49:32 -0500 EST) [User 332508: 0.014/0.041 s] Request help

edas.info/addFollowup.php?errorID=995159#

You are (mostly) on your own

- Credit card
  - liability limited to $50
  - US: mag stripe vs. chip & PIN
- Debit card
  - two days → $50, otherwise $500
- Checks
  - no, your bank does *not* check your signature (or your address)
- Consumer bank account → Regulation E
  - no liability if reported within 60 days
- Small business account
  - No protection, no loss bound
  - ACH fraud common


THIS DOCUMENT HAS A COLORED BACKGROUND AND MICROPRINTING. THE REVERSE SIDE INCLUDES AN ARTIFICIAL WATERMARK.

L 12/26/2006 520384560 0012 3

008808

EDAS Conference Services
1015 Windward Ridge Parkway
Alpharetta, GA 30005
Phone : (800) 499 1888

NetBank
061091977

PER 12/26/2006 10 11 410764962 7135 20 WEIGH

PER 12/26/2006 6 7 450884665

Date : 12/15/2006

PAY TO THE ORDER OF : Kaena Johnson

$ 2230.00

Two Thousand Two Hundred Thirty Dollars and Zero Cents

Dollars

Void after 30 days.

SIGNATURE ON FILE
This check has been authorized
by your depositor.

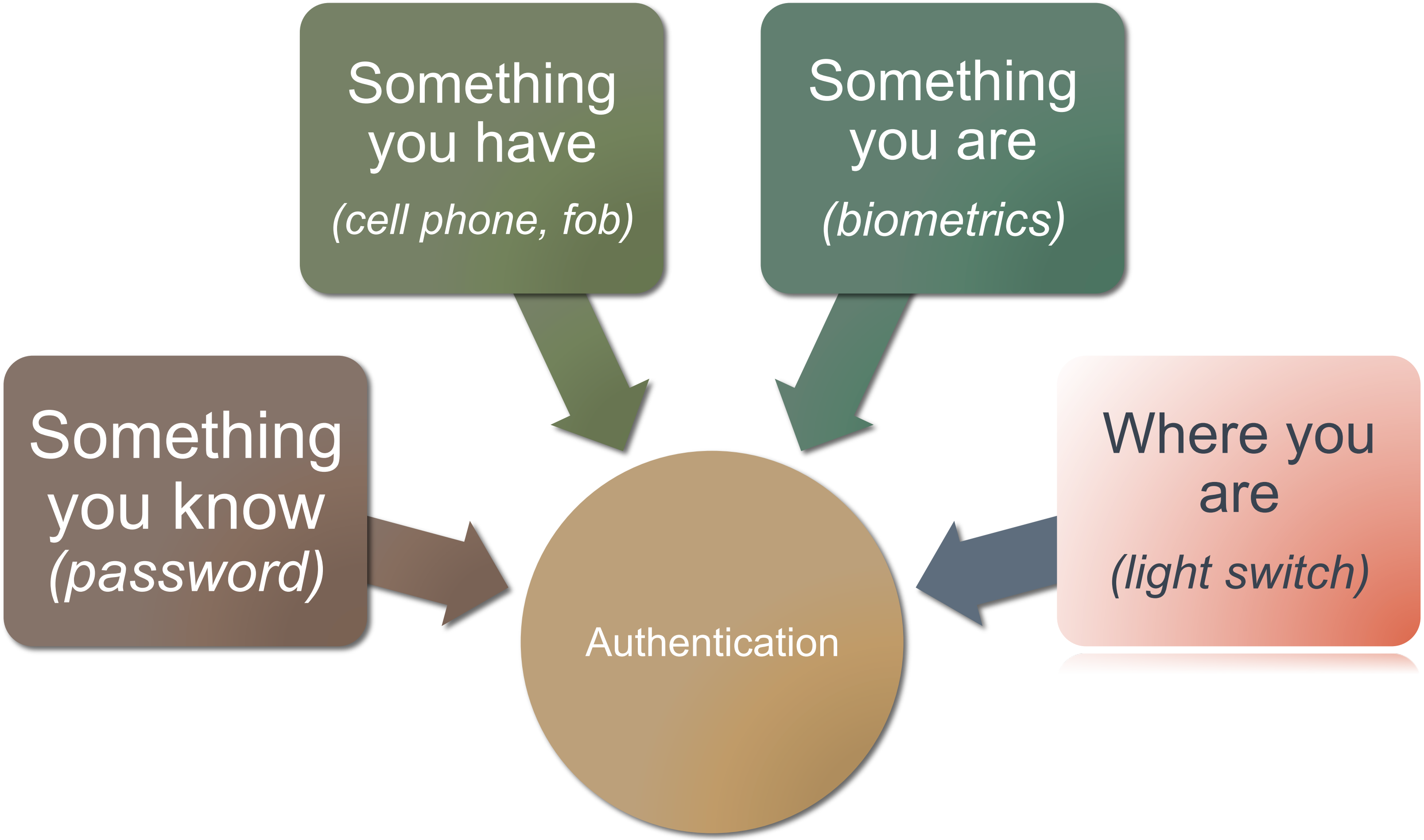
EDAS Conference Serv

Memo : payment

⑈008808⑈ ⑆061091977⑆ 16000034039⑈ ⑈0000223000⑈

AUTHENTICATION

Traditional authentication



Something you have

(cell phone, fob)

Something you are

(biometrics)

Something you know

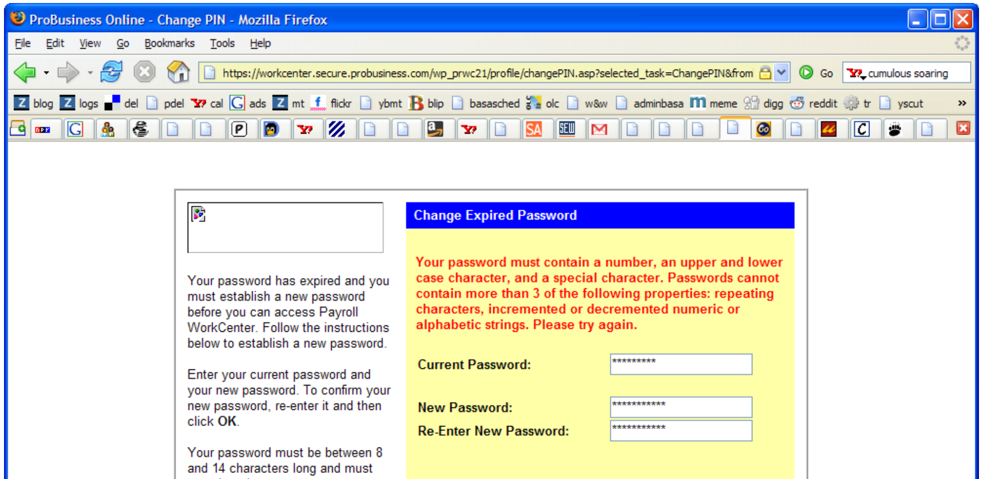
(password)

Where you are

(light switch)

Authentication

Password policies gone amuck


ProBusiness Online - Change PIN - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://workcenter.secure.probusiness.com/wp_prwc21/profile/changePIN.asp?selected_task=ChangePIN&from
Go
cumulous soaring
blog logs del pdel cal ads mt flickr ybmt blip basasched olc w&w adminbasa meme digg reddit tr yscut
Find: berk
Find Next
Find Previous
Highlight
Done

Your password has expired and you must establish a new password before you can access Payroll WorkCenter. Follow the instructions below to establish a new password.

Enter your current password and your new password. To confirm your new password, re-enter it and then click **OK**.

Your password must be between 8 and 14 characters long and must contain at least one upper case letter, one lower case letter, one number and one standard special character (like %, @ or #).

Passwords cannot contain: more than 3 repeating characters, more than 3 incremented or decremented numeric strings or more than 3 incremented or decremented alphabetic strings.

Logon ID and password cannot be the same.

Note: Passwords are case sensitive.

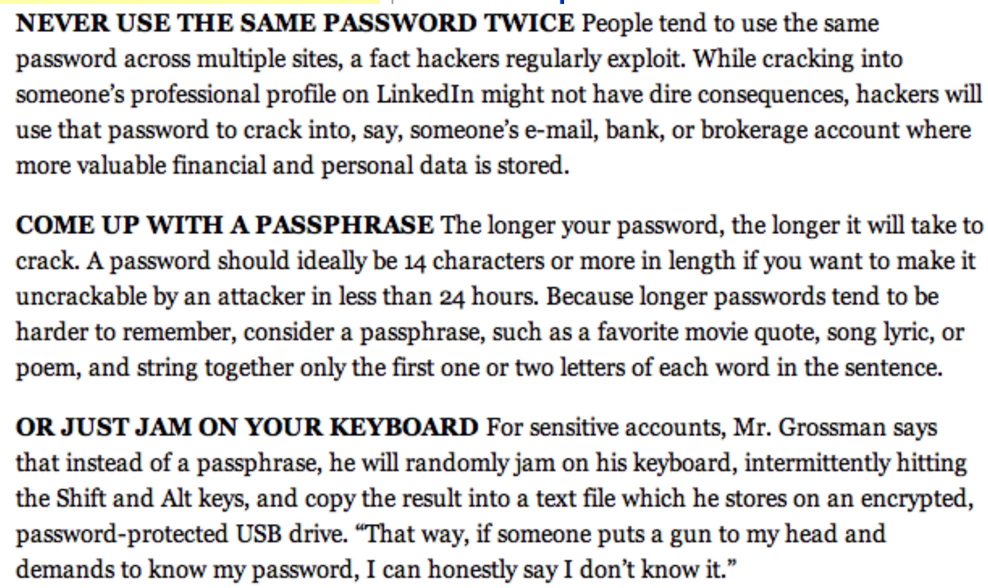
To Cancel this process without changing your password, click **Cancel**.

Change Expired Password

Your password must contain a number, an upper and lower case character, and a special character. Passwords cannot contain more than 3 of the following properties: repeating characters, incremented or decremented numeric or alphabetic strings. Please try again.

Current Password:	*********
New Password:	***********
Re-Enter New Password:	***********

- Contradictory policies
  - Strong passwords don’t work everywhere
- Password expiration
  - and can’t use old one
- Don’t re-use password across sites



NEVER USE THE SAME PASSWORD TWICE People tend to use the same password across multiple sites, a fact hackers regularly exploit. While cracking into someone’s professional profile on LinkedIn might not have dire consequences, hackers will use that password to crack into, say, someone’s e-mail, bank, or brokerage account where more valuable financial and personal data is stored.

COME UP WITH A PASSPHRASE The longer your password, the longer it will take to crack. A password should ideally be 14 characters or more in length if you want to make it uncrackable by an attacker in less than 24 hours. Because longer passwords tend to be harder to remember, consider a passphrase, such as a favorite movie quote, song lyric, or poem, and string together only the first one or two letters of each word in the sentence.

OR JUST JAM ON YOUR KEYBOARD For sensitive accounts, Mr. Grossman says that instead of a passphrase, he will randomly jam on his keyboard, intermittently hitting the Shift and Alt keys, and copy the result into a text file which he stores on an encrypted, password-protected USB drive. “That way, if someone puts a gun to my head and demands to know my password, I can honestly say I don’t know it.”

NY Times, 11/07/2012

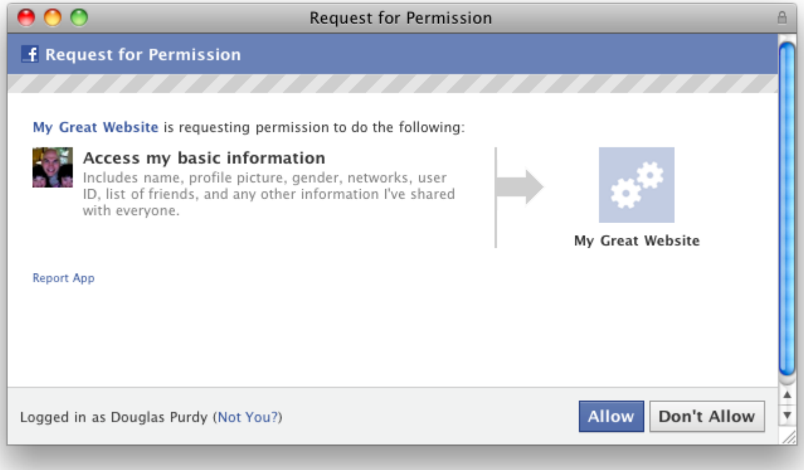
Password advice

- Unless you're the CIA director, writing down passwords is safe
  - you'll pick safer ones if you do
- Stop blaming users → web sites need to tell us what they do
  - bad: plain text, silly rules
  - not much better: hashed
  - good: salted hash, single sign-on
- Impacts password recovery
  - bad: your dog's name
  - not great: send password to email
  - ok: time-limited reset link

More password issues

- With rainbow tables, only length matters
  - 12+ characters likely safe
  - except for dictionary word combinations
  - brute force via GPU: billions of guesses a second
- Always next year: single sign on

OneID



Request for Permission

My Great Website is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.

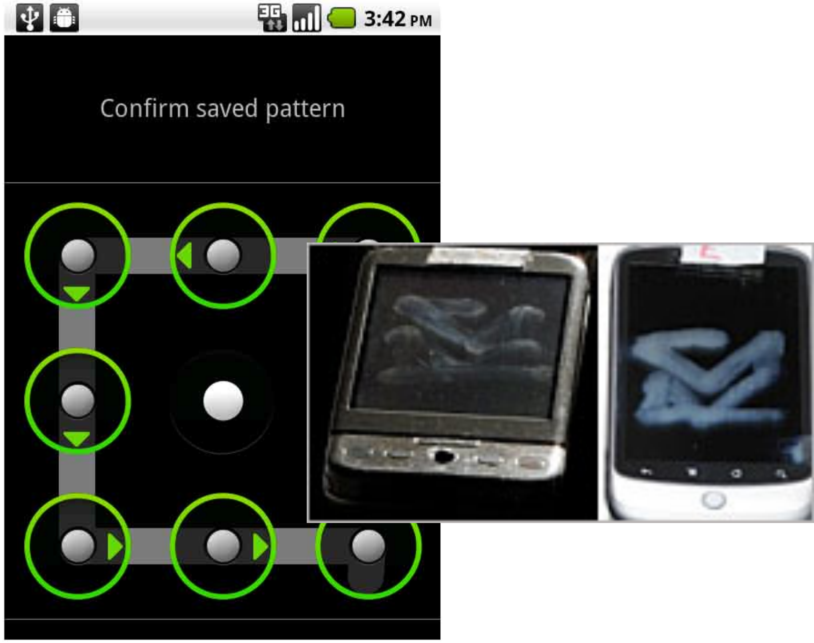
Logged in as Douglas Purdy (Not You?)

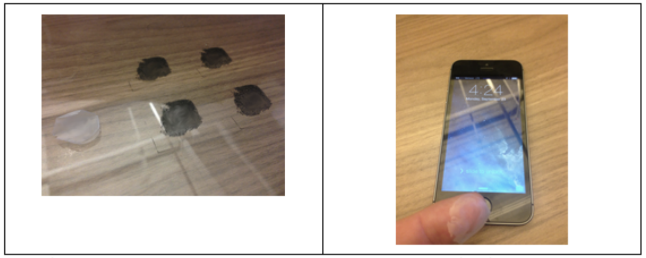
Reduce value of goods

- Particularly single-factor goods
  - if you can't tell that they are gone

What about non-passwords?

- Replacements have been suggested:
  - Swipe pattern (Android)
  - Voice pattern
  - Fingerprints (TouchID)
  - Keyboard typing or swiping
  - Face recognition
- Problems:
  - not generalizable
    - only works on some devices
  - not precisely representable
    - doomed if you have a cold or are in a noisy airport
    - likely need password backup
  - hard to have different ones → bad if clonable
- Useful as supplement for high-value transactions



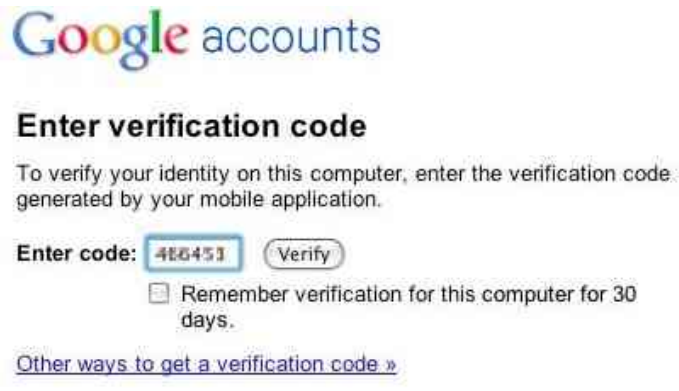


Fake fingerprint alongside transparency prints

Using the fake fingerprint

The convergence to “what you have”

- Two-factor authentication
- Advantages:
    - easy to recognize when lost
    - hard to scale theft (but: see RSA)
    - separate data path
        - voice path vs. data path
        - postal mail
    - related: host recognition (e.g., via cookies)



Google accounts

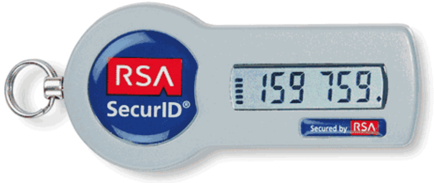
Enter verification code

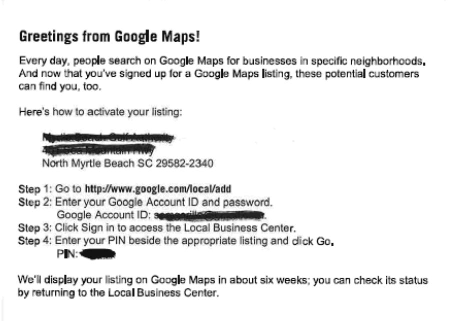
To verify your identity on this computer, enter the verification code generated by your mobile application.

Enter code: 486453

□ Remember verification for this computer for 30 days.

Other ways to get a verification code »





Greetings from Google Maps!

Every day, people search on Google Maps for businesses in specific neighborhoods. And now that you've signed up for a Google Maps listing, these potential customers can find you, too.

Here's how to activate your listing:

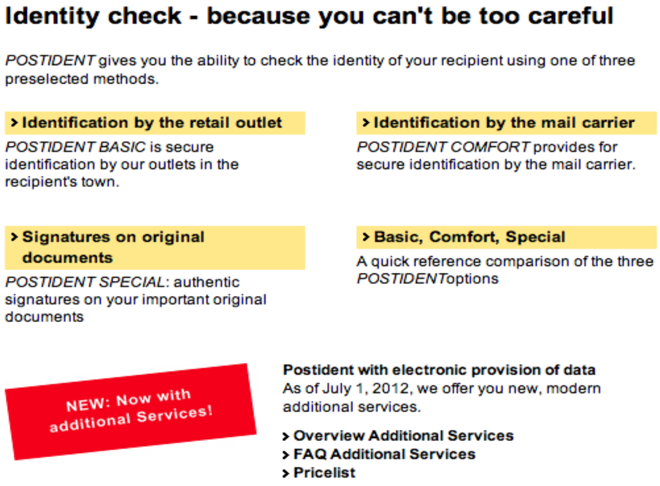
[redacted]
North Myrtle Beach SC 29582-2340

Step 1: Go to **http://www.google.com/local/add**
Step 2: Enter your Google Account ID and password.
Google Account ID: [redacted].
Step 3: Click Sign in to access the Local Business Center.
Step 4: Enter your PIN beside the appropriate listing and click Go.
PIN: [redacted]

We'll display your listing on Google Maps in about six weeks; you can check its status by returning to the Local Business Center.

Provide physical validation services

- Goals:
  - make scaling hard for bad guy
  - increase risk of arrest
  - make geography matter
- But generally not integrated with digital processes!



Identity check - because you can't be too careful

POSTIDENT gives you the ability to check the identity of your recipient using one of three preselected methods.

> Identification by the retail outlet

POSTIDENT BASIC is secure identification by our outlets in the recipient's town.

> Identification by the mail carrier

POSTIDENT COMFORT provides for secure identification by the mail carrier.

> Signatures on original documents

POSTIDENT SPECIAL: authentic signatures on your important original documents

> Basic, Comfort, Special

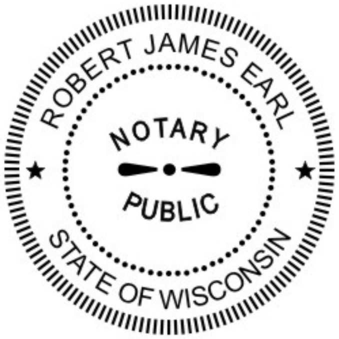
A quick reference comparison of the three *POSTIDENT*options

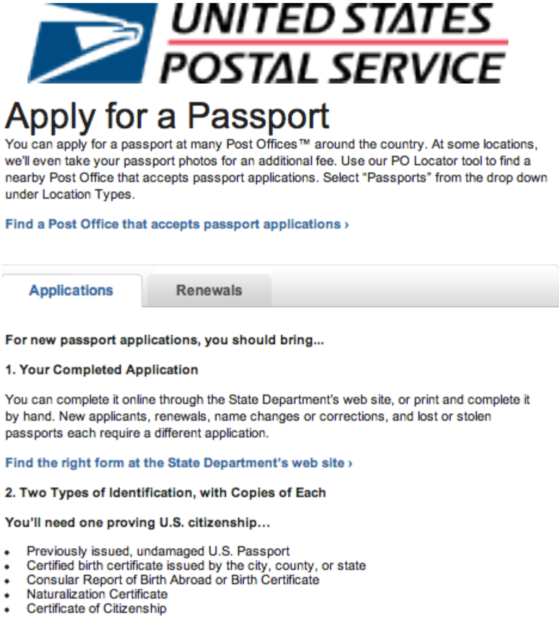
NEW: Now with additional Services!

Postident with electronic provision of data

As of July 1, 2012, we offer you new, modern additional services.

> Overview Additional Services
> FAQ Additional Services
> Pricelist





Apply for a Passport

You can apply for a passport at many Post Offices™ around the country. At some locations, we'll even take your passport photos for an additional fee. Use our PO Locator tool to find a nearby Post Office that accepts passport applications. Select "Passports" from the drop down under Location Types.

Find a Post Office that accepts passport applications ›

For new passport applications, you should bring...

1. Your Completed Application

You can complete it online through the State Department's web site, or print and complete it by hand. New applicants, renewals, name changes or corrections, and lost or stolen passports each require a different application.

Find the right form at the State Department's web site ›

2. Two Types of Identification, with Copies of Each

You'll need one proving U.S. citizenship...

- Previously issued, undamaged U.S. Passport
- Certified birth certificate issued by the city, county, or state
- Consular Report of Birth Abroad or Birth Certificate
- Naturalization Certificate
- Certificate of Citizenship

SECURING THE INTERNET

We must make the Internet secure!

Application layer

- knows the what & who

Transport layer: TLS, DTLS

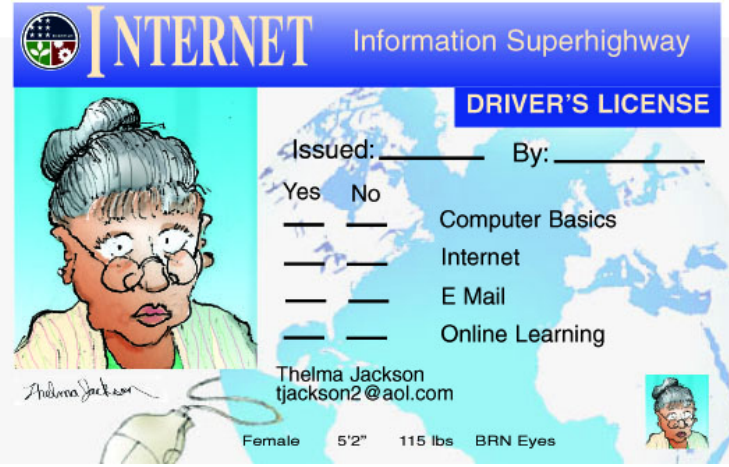
- certificate validation often wrong
- no client certificates (domain vs. user)
- integrated transport & security layer?

Internet layer

- deployability
- doesn’t know user & desired operation
- changes with mobility
- IP layer as introducer → by definition, parties may not know each other
- → secure *infrastructure*

Securing the Internet – once and for all!

- Dream of a security layer that lets everybody else do nothing
- Suggested: “Internet passport”
  - no more unauthenticated packets!
  - what about compromised machines?
- Possible:
  - “don’t talk to me unless I talked to you”
  - → permission-based sending
  - most useful for small-group DOS attacks
    - but most are now trickle attacks
  - keep out packets at coarse level
    - “not interested in packets from Elbonia”
      - but easily spoofed



INTERNET Information Superhighway

DRIVER'S LICENSE

Issued: ______ By: ______

Yes No

__ __ Computer Basics

__ __ Internet

__ __ E Mail

__ __ Online Learning

Thelma Jackson

tjackson2@aol.com

Female 5'2" 115 lbs BRN Eyes

Cause of death for the next big thing

	QoS	multi-cast	mobile IP	active networks	IPsec	IPv6
not manageable across competing domains	✝	✝	✝	✝		
not configurable by normal users (or apps writers)	✝			✝	✝	
no business model for ISPs	✝	✝	✝	✝	✝	✝
no initial gain	✝	✝	✝	✝		✝
80% solution in existing system	✝	✝	✝	✝	✝	✝ (NAT)
increase system vulnerability	✝	✝	✝	✝		

Secure key identifiers

- Security by:
  - return routability
  - cryptographic proof of ownership
  - keeping them secret (SSN)

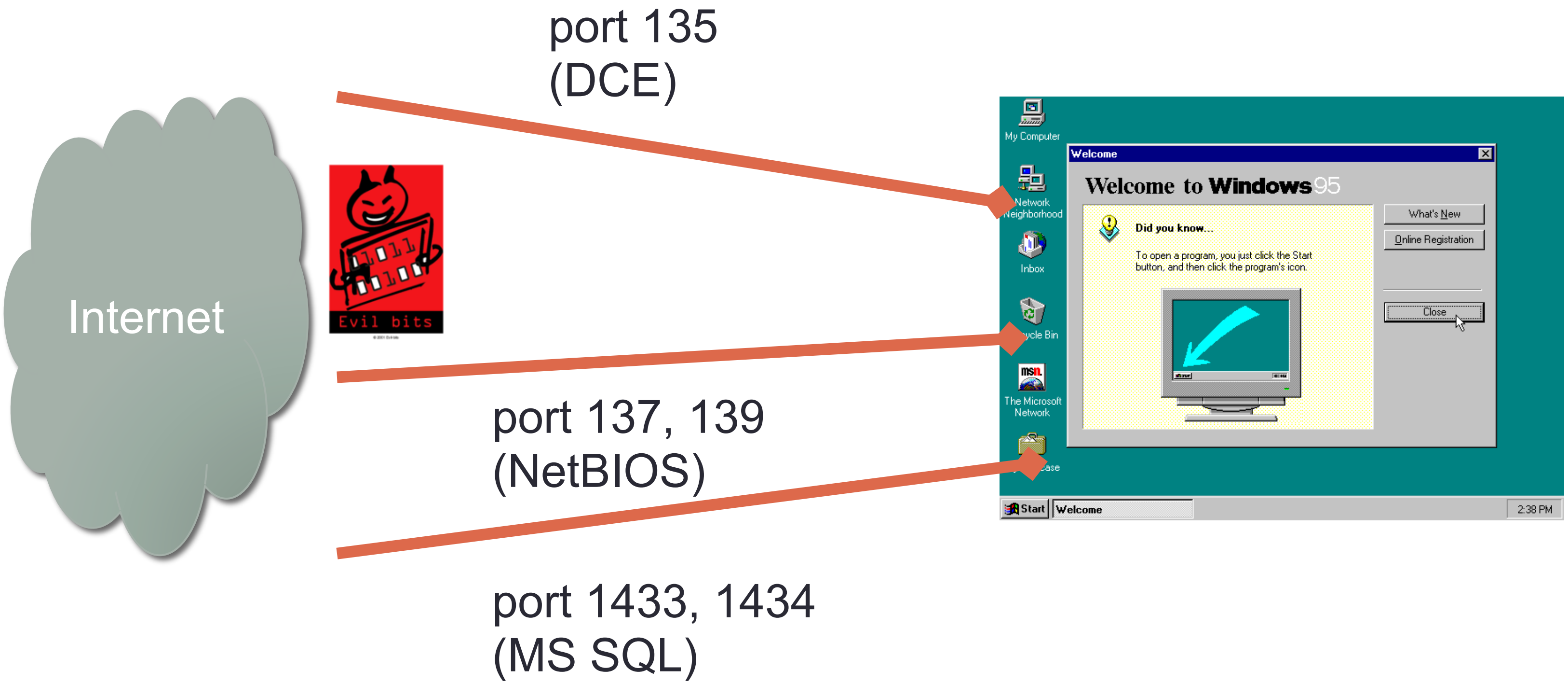
Identifier	Proof of ownership	Spoofable	Critical for
IP address	RR, RPKI (?)	egress filtering (RFC 3013)	everything…
AS number	RPKI?	yes (BGP)	routing
domain name	TLS	TLS failures → DANE	web sites
email address	RR	mostly	password recovery
phone number	RR	caller-ID spoofing	2-factor authentication
location	?	yes	authentication

Avoid single-failure = catastrophic failure

- Download the wrong application ➔ bank account gone
- Attacker advantage: one flaw, hundreds of thousands of victims
- → Make it hard to scale attacks
  - require access to physical world
  - multiple paths that are unpredictable to far-away third party
  - Honey pots (e.g., trap spam senders)
- System design:
  - separate systems for high-value transactions
    - separate web browser
    - separate VM
    - single-purpose computer
    - second independent path: SMS

SECURING END SYSTEMS

The old attack model

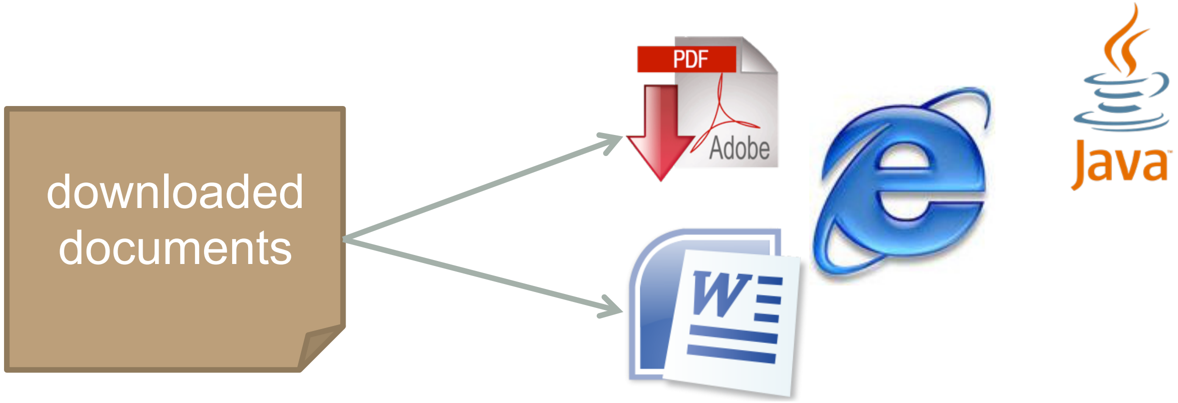


Welcome to Windows95

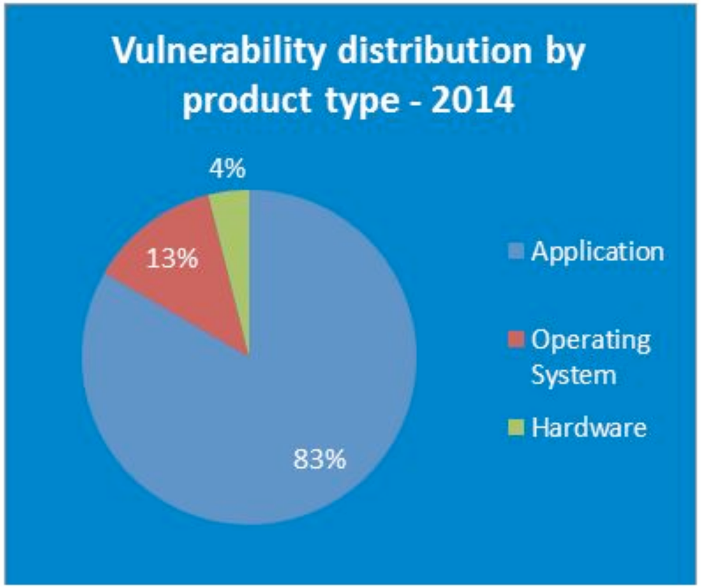
Did you know...

To open a program, you just click the Start button, and then click the program's icon.

… and now

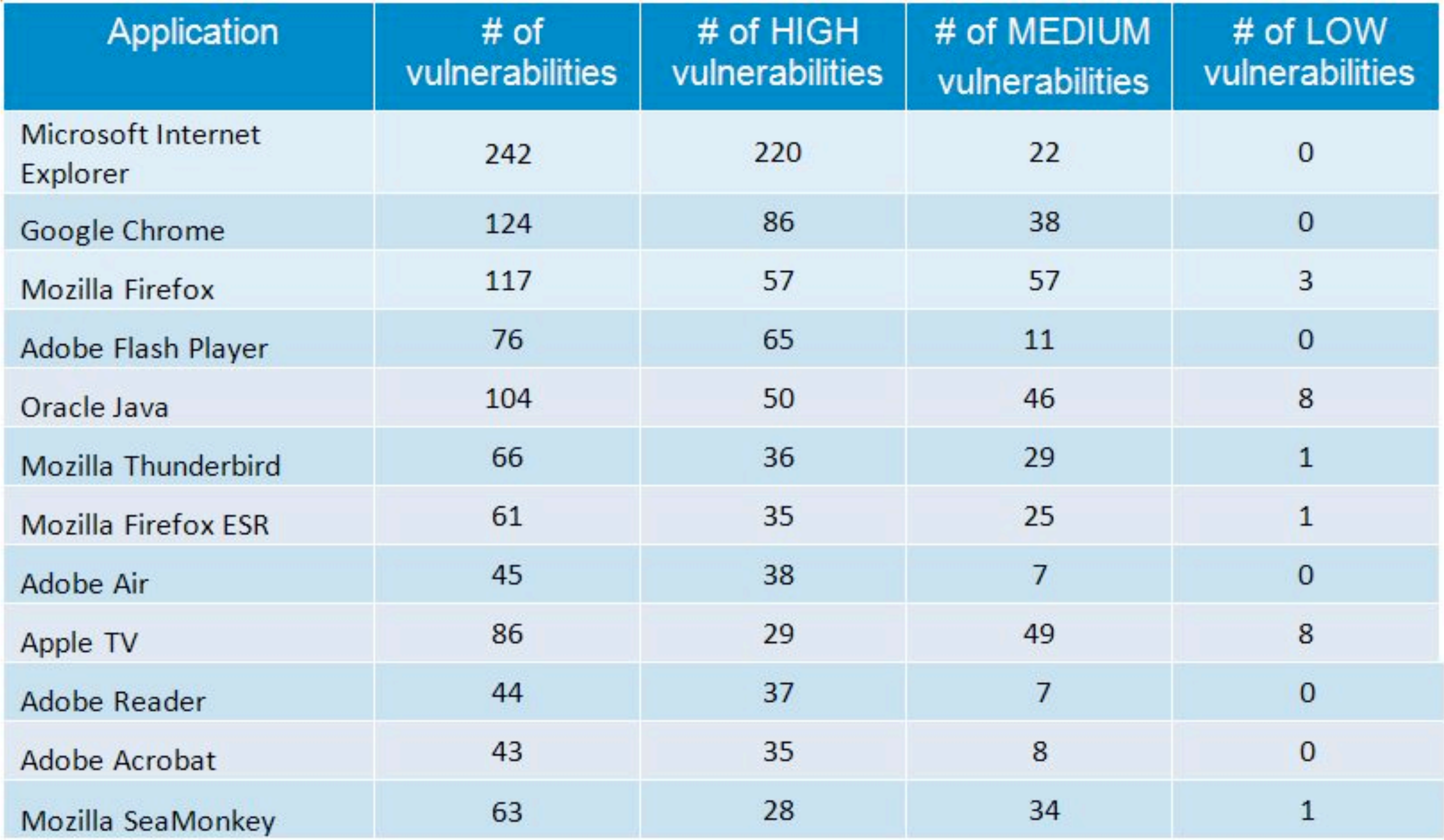


downloaded documents



Vulnerabilities 2014

dubious metric?



Application	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Microsoft Internet Explorer	242	220	22	0
Google Chrome	124	86	38	0
Mozilla Firefox	117	57	57	3
Adobe Flash Player	76	65	11	0
Oracle Java	104	50	46	8
Mozilla Thunderbird	66	36	29	1
Mozilla Firefox ESR	61	35	25	1
Adobe Air	45	38	7	0
Apple TV	86	29	49	8
Adobe Reader	44	37	7	0
Adobe Acrobat	43	35	8	0
Mozilla SeaMonkey	63	28	34	1

What can be done?

- Harden key libraries
  - protocols (HTTP, SMTP, IMAP, SIP, …)
  - file type parsing
  - → fuzzing
- Separate parsing & system access via pipe
  - e.g., Google Chrome
- Separate VMs for enterprise applications (e.g., Docker)
  - allow separate IP address → filtering
- Self-learning security systems
  - MySQL: “I always get database queries from 128.59.16.10”

What can be done?

- Restrict privileges
  - Android: each app has separate user ID
  - Permission restriction
    - App store, rather than browser, for installing software
    - No need to store files in system areas
    - Limited system permissions
      - harder with HTML5, WebRTC, SVG, …
- Separate trusted hardware
  - **not** programmable
  - for high-value interactions
  - based on physical proximity

All systems must update automatically

- Manual updates → compromise (see Adobe Flash)
  - Microsoft “patch Tuesdays”
- “*Evergreen browsers*”: Firefox, Chrome
- MacOS transitioning to automatic updates
- yum on CentOS and RedHat EL
- Google policy on responsible disclosure

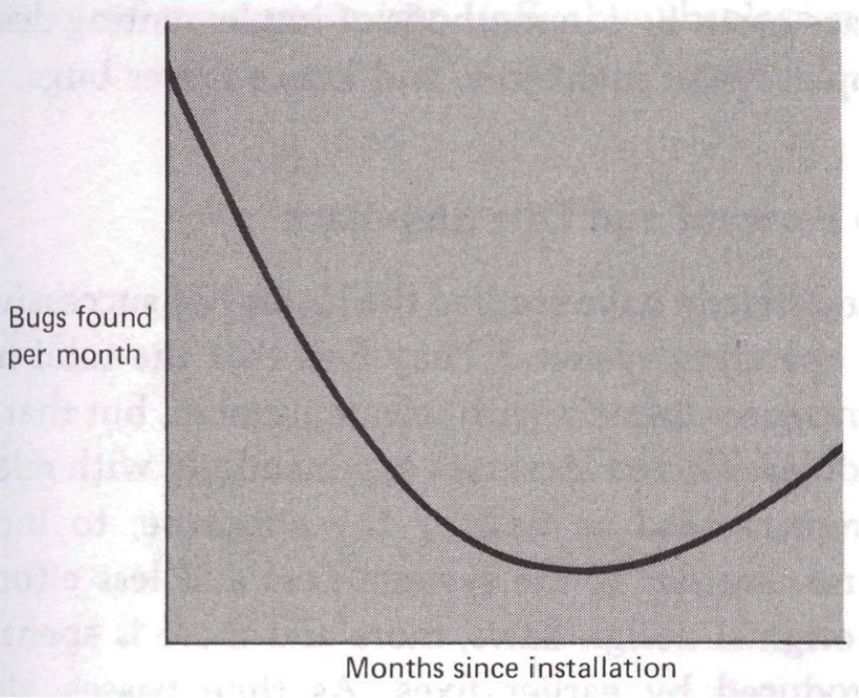
Software Lifecycle

- We are used to throwing computers away
  - Your phone, laptop, desktops, etc.
  - We've learned through great pain that we **must** keep them updated
- But we now build long lived devices and systems with computers inside, that are Internet connected
  - Your thermostats, home theater, home router, home theater, security cameras, light bulbs, etc. Soon car, refrigerators, coffee makers...
  - Installation costs often greatly exceed cost of the computer
- Some devices have potential lifetimes measured in decades
  - *These timescales are long relative to human organizations*
  - We've presumed we can "forget about these boxes"
  - Is this safe? NO! The SCADA problem writ large

Familiarity Breeds Contempt:

The Honeymoon Effect and the Role of Legacy Code in Zero-day Vulnerabilities

By Sandy Clark, Stefan Frei, Matt Blaze, Jonathan Smith, ACSAC '10



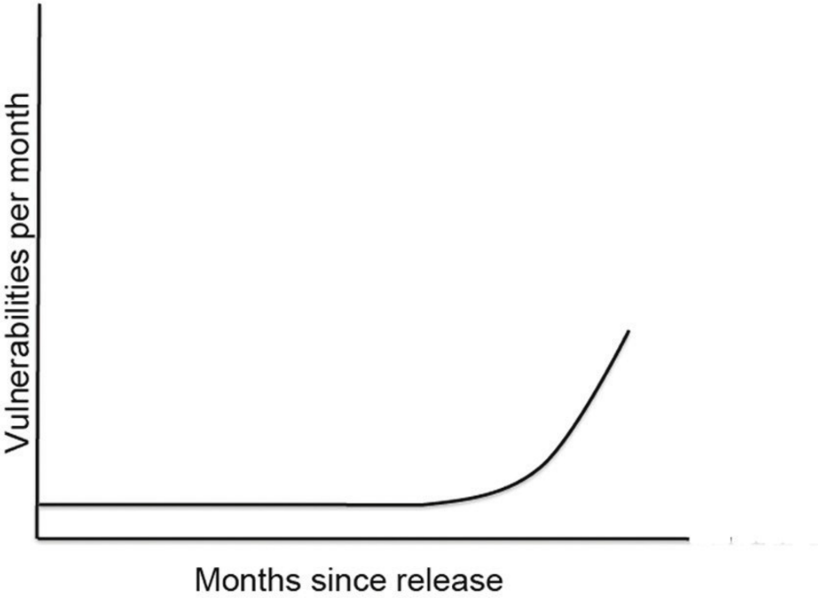


Figure 1

Home Routers, Modems, etc.

- Most important, as they are both MITM and your lifeline
- We now depend on our Internet service
  - e.g. POTS (wired telephones) are doomed: you'd like your phone to work in an emergency
- Brand new devices unmaintained and unpatched
  - **New devices start with 4 year old code!**
- Firmware is usually not updated after ~1 year after sale by vendor, after the crash rate diminishes, then rots
  - For most, you have to manually update them, and are even never notified of updates, if they even exist
- Embedded devices (e.g. your Nest thermostats) are no different than routers, except they are not on your path to the rest of the world (and are updated, at least for now...)

Wake Up Calls

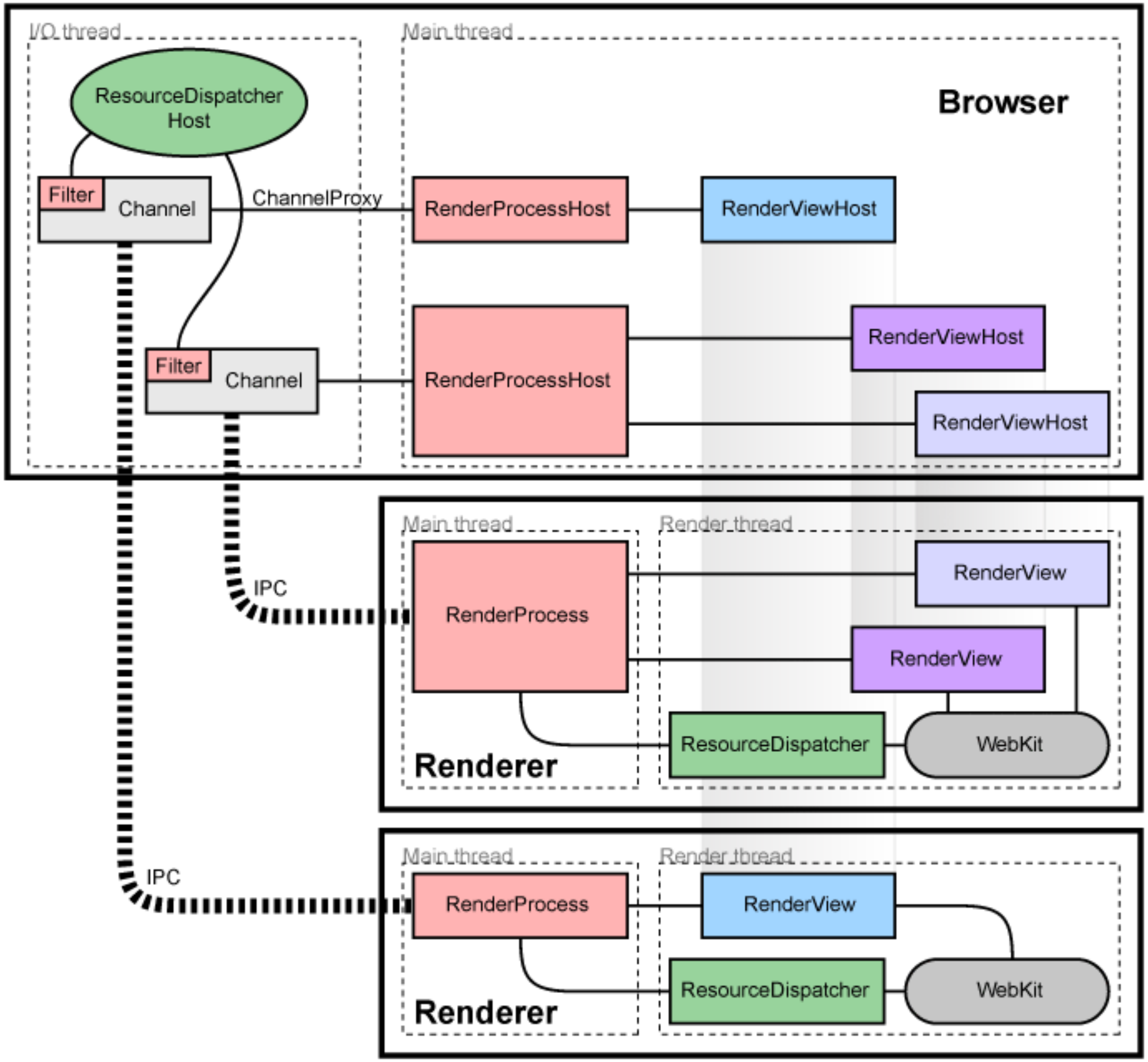
Bad guys have noticed these devices are vulnerable

- Research demonstrating *single* vulnerabilities that affect > half of the tested home routers
- A few examples:
  - DNSchanger attacked home routers as well as hosts
  - 4.5 million DSL routers in Brazil
  - TheMoon worm: most models of Linksys routers
  - Heartbleed...
- It's a matter of when, rather than if, we have a big, big problem, if we don't already...

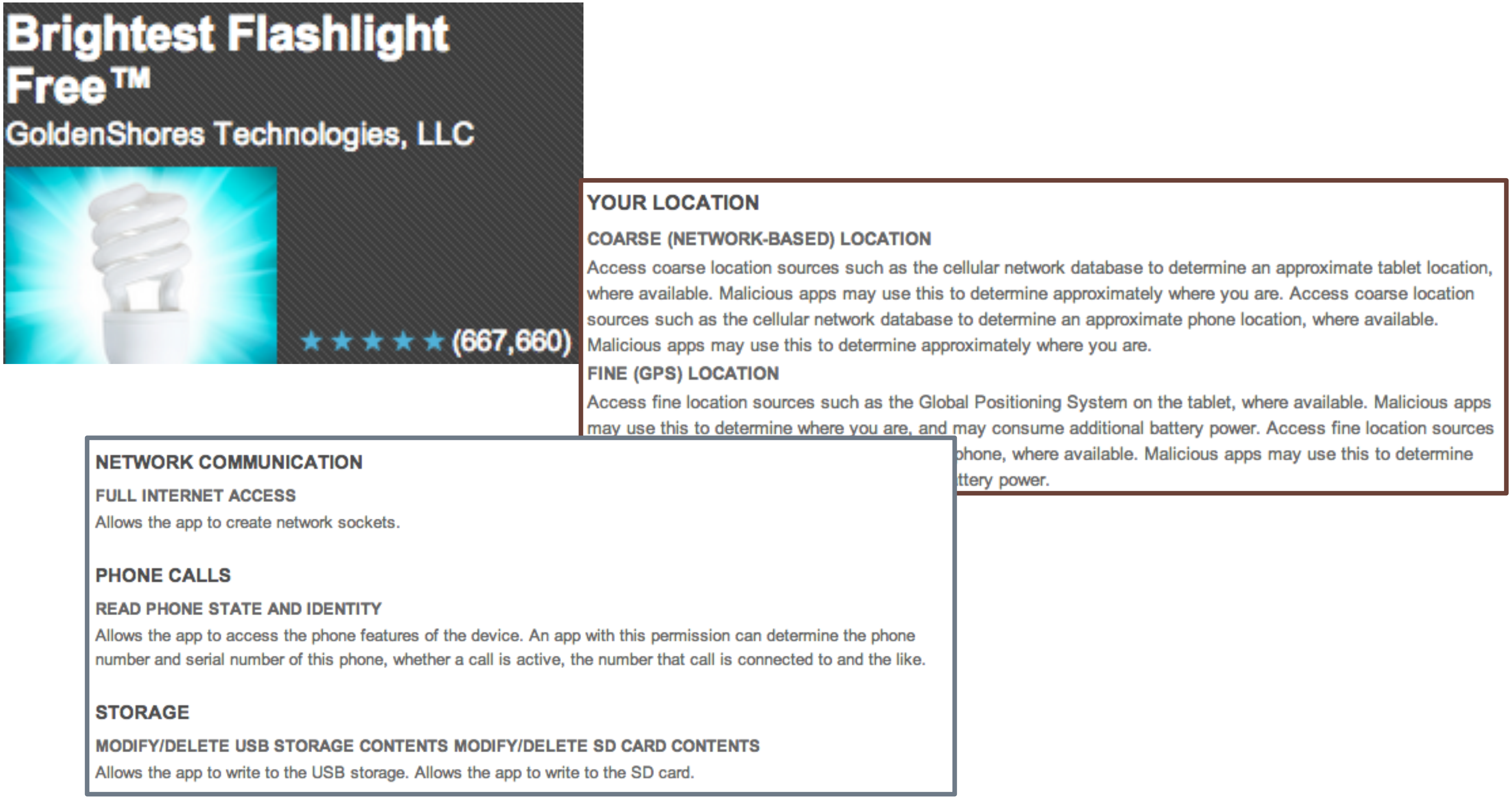
NTP reflection attack

Jim Gettys (June 2014)

Design pattern: process separation



App permissions are not sufficient



Brightest Flashlight Free™

GoldenShores Technologies, LLC

★★★★★ (667,660)

YOUR LOCATION

COARSE (NETWORK-BASED) LOCATION

Access coarse location sources such as the cellular network database to determine an approximate tablet location, where available. Malicious apps may use this to determine approximately where you are. Access coarse location sources such as the cellular network database to determine an approximate phone location, where available. Malicious apps may use this to determine approximately where you are.

FINE (GPS) LOCATION

Access fine location sources such as the Global Positioning System on the tablet, where available. Malicious apps may use this to determine where you are, and may consume additional battery power. Access fine location sources

phone, where available. Malicious apps may use this to determine

ttery power.

NETWORK COMMUNICATION

FULL INTERNET ACCESS

Allows the app to create network sockets.

PHONE CALLS

READ PHONE STATE AND IDENTITY

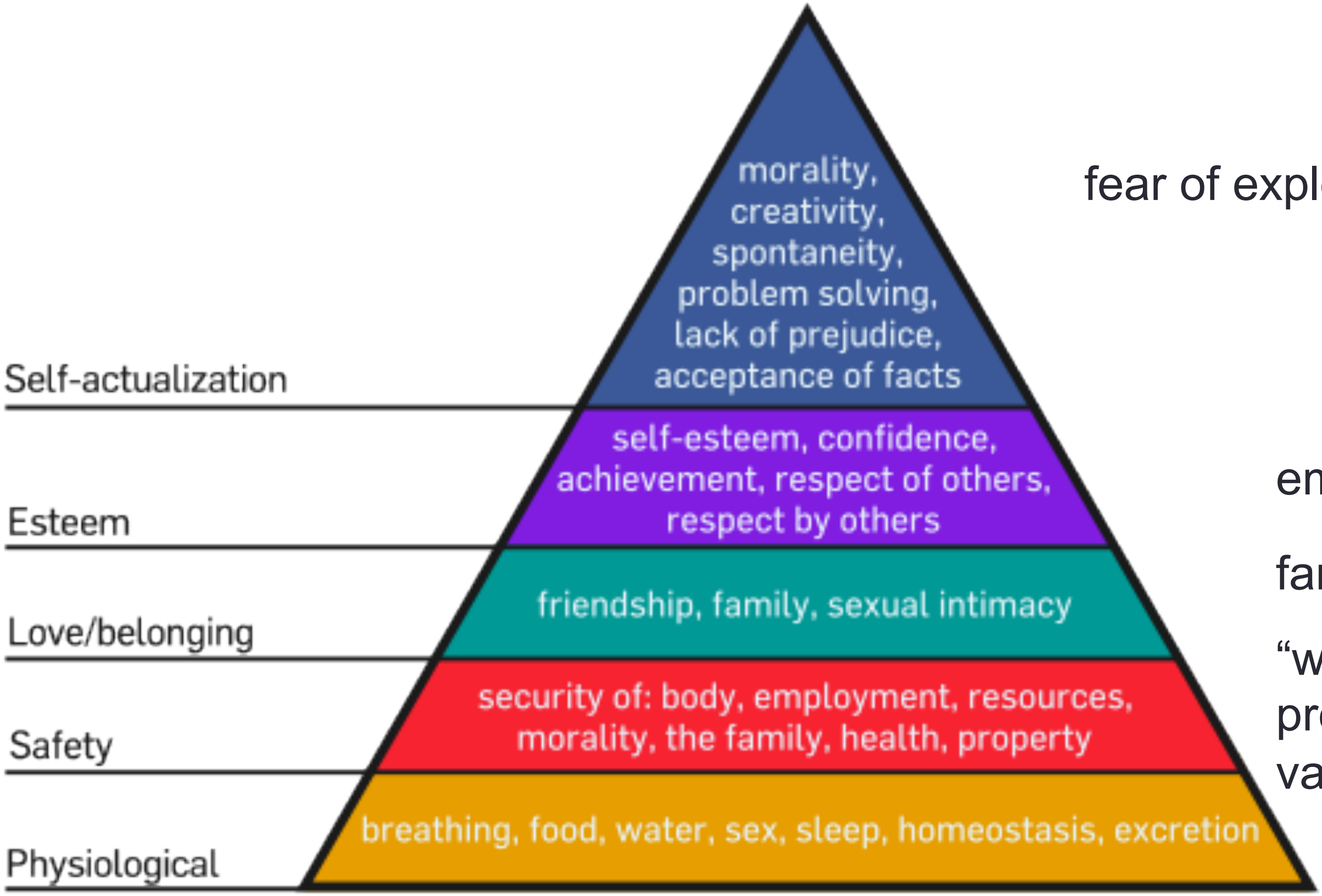
Allows the app to access the phone features of the device. An app with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and the like.

STORAGE

MODIFY/DELETE USB STORAGE CONTENTS MODIFY/DELETE SD CARD CONTENTS

Allows the app to write to the USB storage. Allows the app to write to the SD card.

Privacy threats


morality, creativity, spontaneity, problem solving, lack of prejudice, acceptance of facts
Self-actualization
self-esteem, confidence, achievement, respect of others, respect by others
Esteem
friendship, family, sexual intimacy
Love/belonging
security of: body, employment, resources, morality, the family, health, property
Safety
breathing, food, water, sex, sleep, homeostasis, excretion
Physiological

fear of exploration

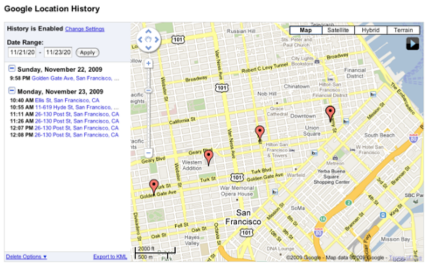
embarrassment

family secrets

“we regret to inform you”
pre-existing condition
vacation burglary
stalking

Privacy

- Difficulty of defining privacy
  - specific threats vs. just fear of threat
  - current vs. future (e.g., job search)
- Emphasis on data gathering unhelpful
  - → same information can be used for low-risk and high-risk activities
- IETF GEOPRIV approach:
  - how long is data stored?
  - is it shared with third parties?
    - (but what are third parties?)



Google Location History

History is Enabled Change Settings

Date Range:
11/21/20 - 11/23/20 Apply

Sunday, November 22, 2009
9:58 PM Golden Gate Ave, San Francisco, ...

Monday, November 23, 2009
10:40 AM Ellis St, San Francisco, CA
10:55 AM 11-619 Hyde St, San Francisco, ...
11:11 AM 26-130 Post St, San Francisco, CA
11:26 AM 26-130 Post St, San Francisco, CA
12:07 PM 26-130 Post St, San Francisco, CA
12:08 PM 26-130 Post St, San Francisco, CA

Delete Options ▾ Export to KML

Map
Satellite
Hybrid
Terrain
San Francisco

FOR KIDS
ADS NO
SOCIAL NO
LOCATION NO
WEB YES
PURCHASE NO
AGES 3+

Privacy – other approaches

- Hiding & obfuscation
  - e.g., pretend that location is unavailable
  - fuzz location
- Restrict sensitive information to approved purposes
  - expose location to well-known ad network, not unknown
- Third-party privacy evaluation
- FTC Section 5 enforcement (“unfair or deceptive practices”)

Improving network infrastructure security

- FCC + industry for six months → three critical threats to the Internet:
  - Domain Name System security
  - Routing security
  - Botnets
- Specific voluntary recommendations approved by CSRIC in March 2011 to advance deployment of DNSSEC, BGPSEC, and a domestic ISP Code of Conduct to fight botnets.
- Nine of the largest ISPs, representing nearly 90% of the domestic user base, publicly announced their intent to deploy the recommendations.
- Next step: measure deployment & impact → *Measuring Broadband America*

What can be done?

insecure device

secure device

TÜVRheinland®
CERTIFIED

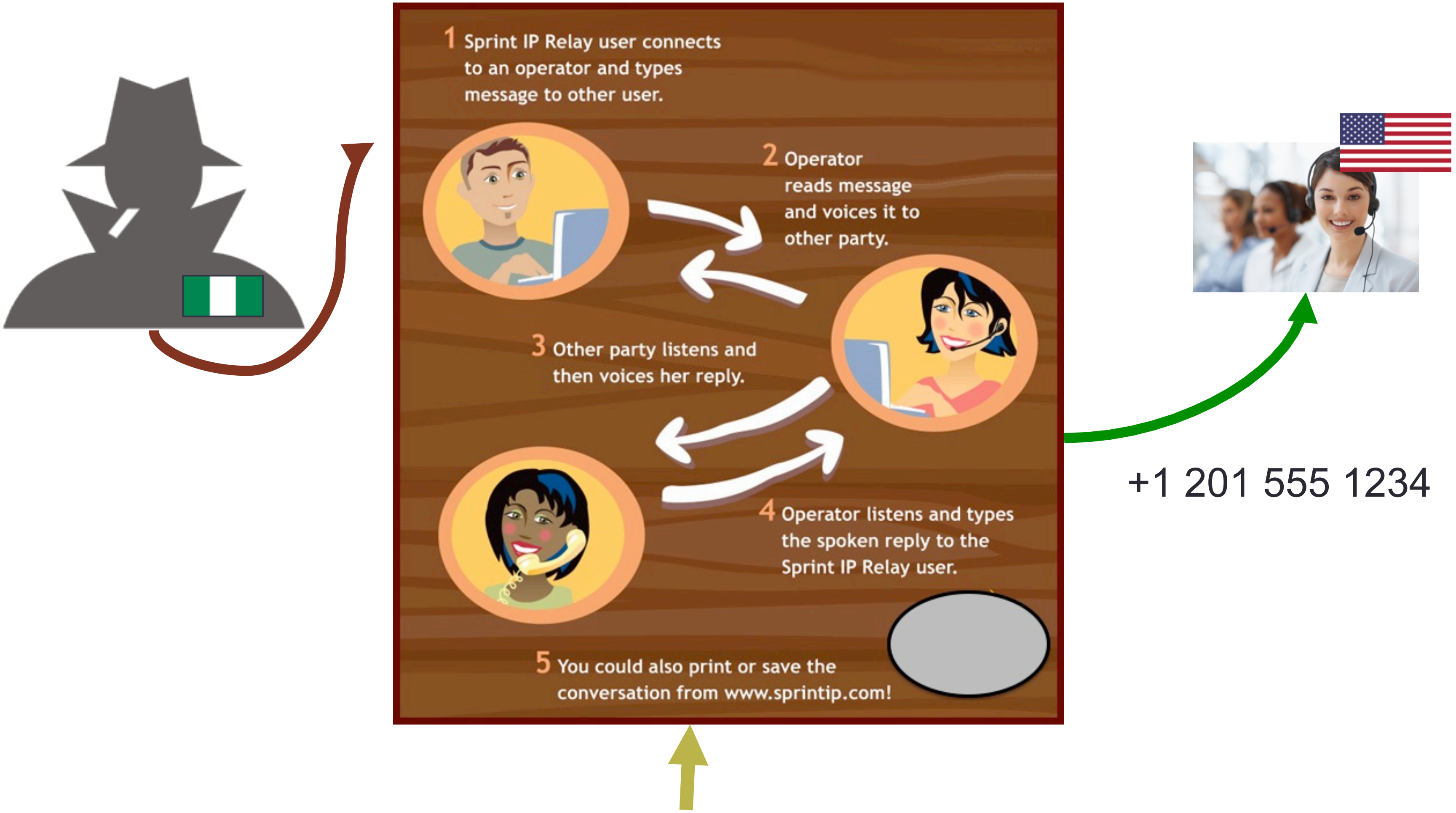
UL®

pci DSS COMPLIANT

?

SECURITY BEYOND VIRUSES AND PHISHING: FRAUD & HUMAN DOS ATTACKS

Fraud in TRS (text relay service)



1 Sprint IP Relay user connects to an operator and types message to other user.

2 Operator reads message and voices it to other party.

3 Other party listens and then voices her reply.

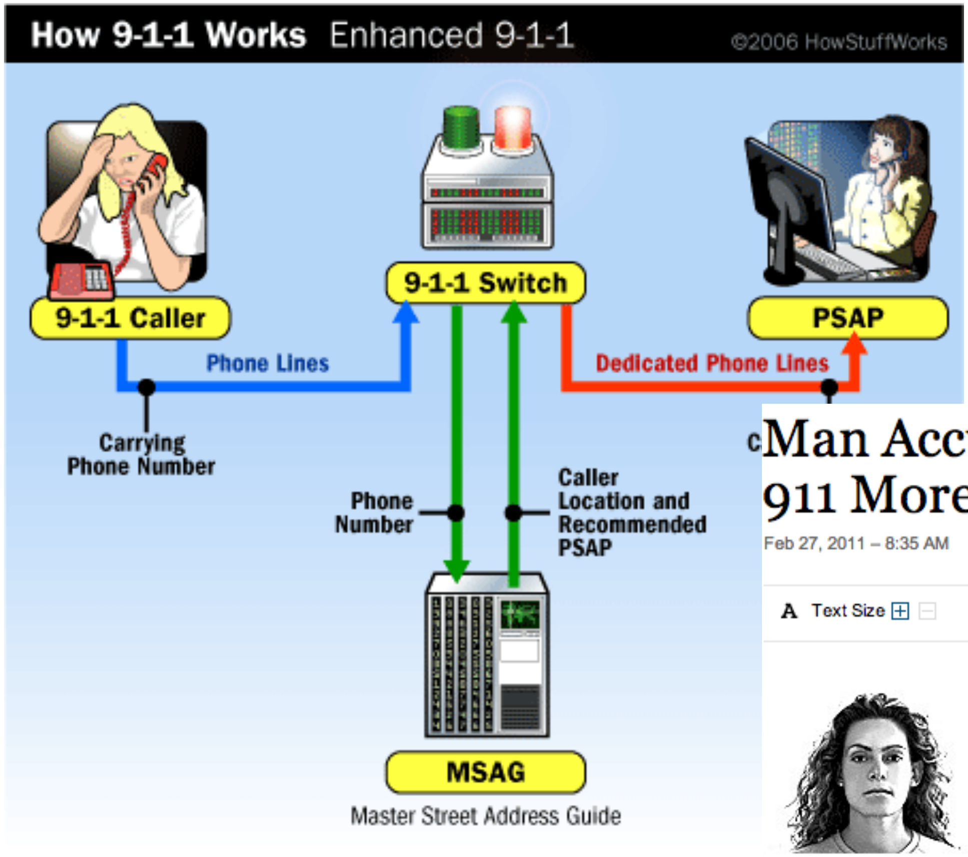
4 Operator listens and types the spoken reply to the Sprint IP Relay user.

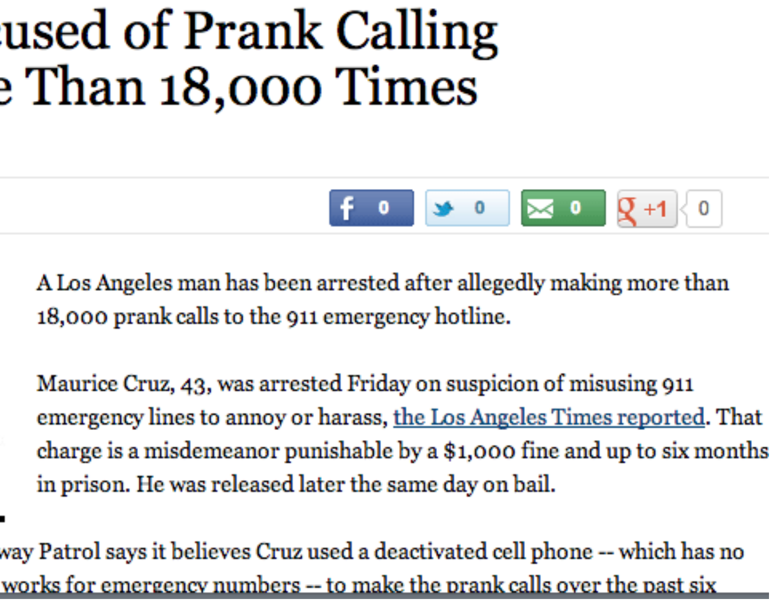
5 You could also print or save the conversation from www.sprintip.com!

+1 201 555 1234

TTY	CTS	IP CTS	STS	VRS 1	VRS 2	VRS 3	IP
$ 2.0304	$ 1.7730	$ 1.7730	$ 3.1614	$ 6.2390	$ 6.2335	$ 5.0668	$ 1.2855

DOS attacks on humans: 9-1-1





Man Accused of Prank Calling 911 More Than 18,000 Times

Feb 27, 2011 – 8:35 AM

Lauren Frayer
Contributor

A Los Angeles man has been arrested after allegedly making more than 18,000 prank calls to the 911 emergency hotline.

Maurice Cruz, 43, was arrested Friday on suspicion of misusing 911 emergency lines to annoy or harass, the Los Angeles Times reported. That charge is a misdemeanor punishable by a $1,000 fine and up to six months in prison. He was released later the same day on bail.

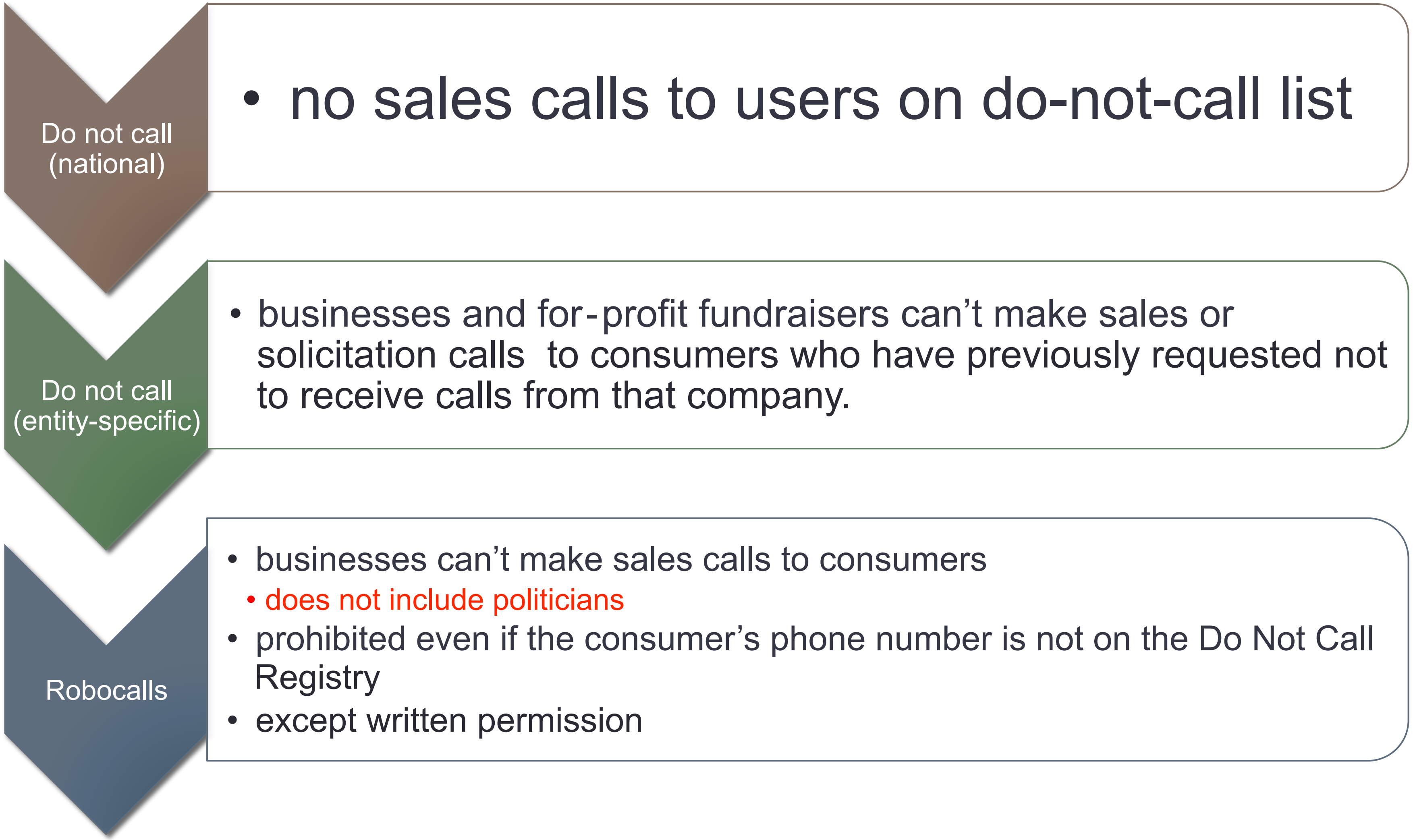
The California Highway Patrol says it believes Cruz used a deactivated cell phone -- which has no service plan but still works for emergency numbers -- to make the prank calls over the past six

Conclusion

- Internet security is a *systems* problem, not (primarily) a crypto or protocol problem
- Treat security as system failures → redundancy, time-to-repair
- Don't wait for the Internet to be secure
- Global optimization:
  - change processes
  - encourage transparency and informed consumer choice
  - economics: externalities – make cause of problem bear the cost

ROBOCALLS & CALLER-ID SPOOFING

The Telemarketing Sales Rule: Three Protections



Do not call (national)

- no sales calls to users on do-not-call list

Do not call (entity-specific)

- businesses and for-profit fundraisers can't make sales or solicitation calls to consumers who have previously requested not to receive calls from that company.

Robocalls

- businesses can't make sales calls to consumers
  - does not include politicians
- prohibited even if the consumer's phone number is not on the Do Not Call Registry
- except written permission

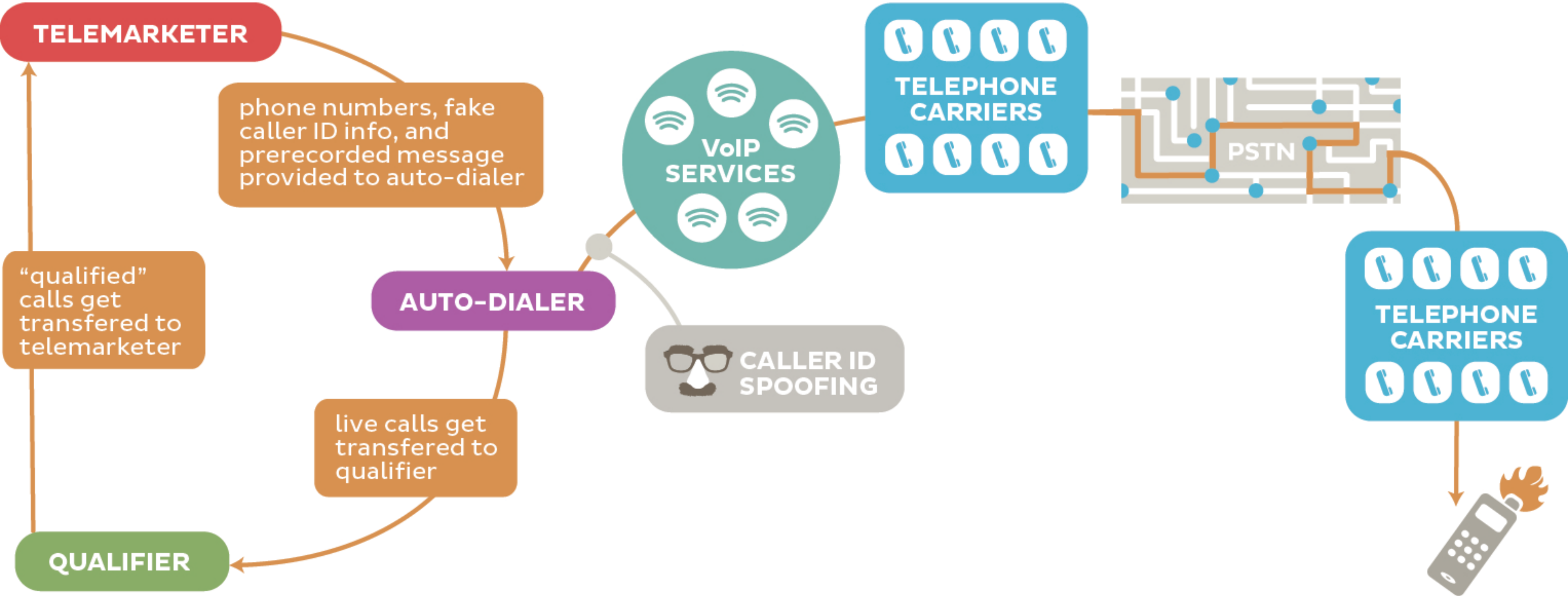
FTC (Will Maxson, 2012)

What calls are **not** covered?

- Most business to businesses telemarketing
- Debt collection calls
- Customer service or customer satisfaction calls
- Market research/survey calls (only if no sales pitch)
- Polling/political calls (get out the vote, contribution requests)
- Calls made by companies subject to special federal /state regulation (banks, phone companies, insurance companies)
- Robocalls delivering a healthcare message made by or for a covered entity, as defined by the HIPAA Privacy Rule

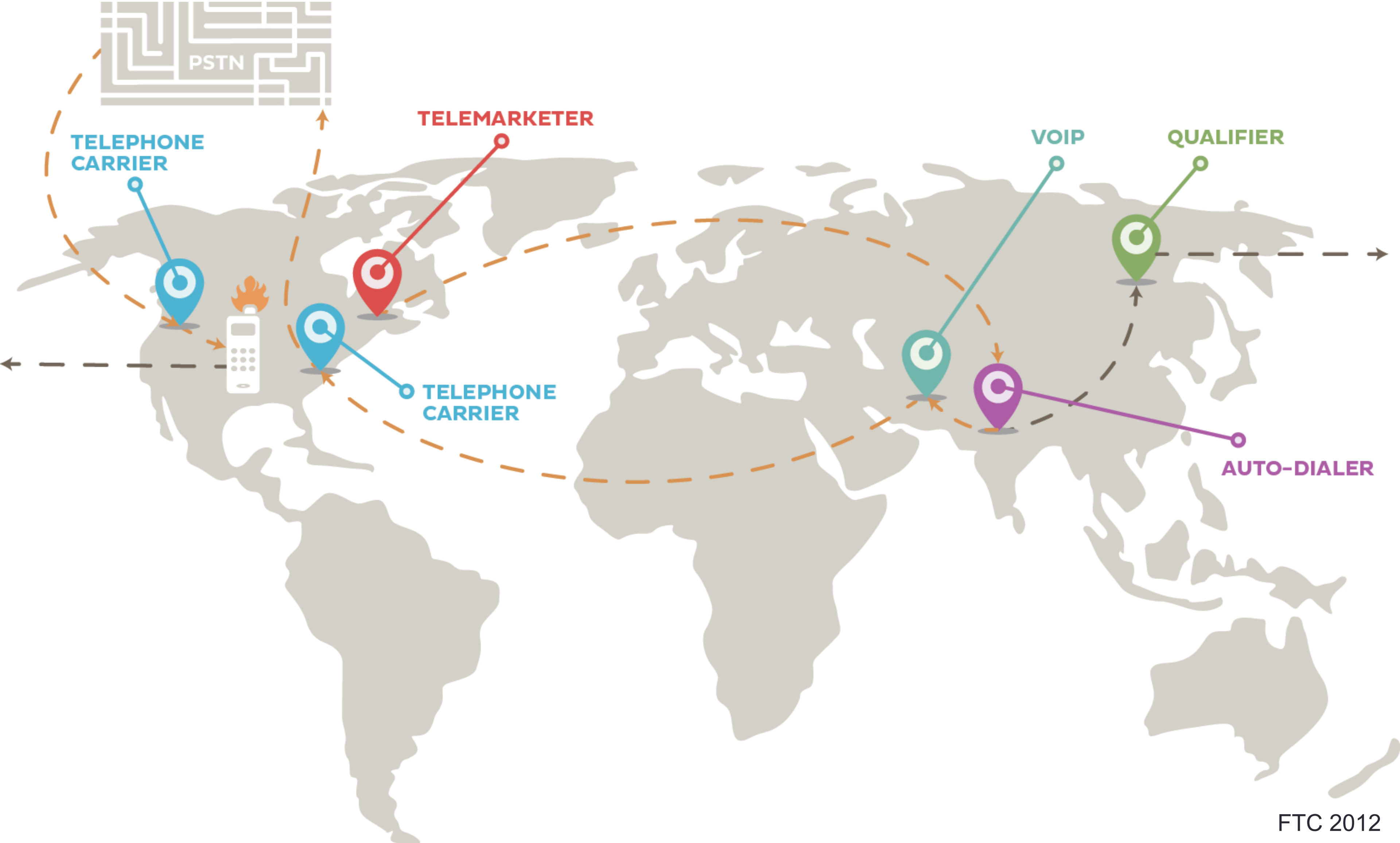
FTC (Will Maxson, 2012)

How do robocalls work?


TELEMARKETER
phone numbers, fake caller ID info, and prerecorded message provided to auto-dialer
AUTO-DIALER
live calls get transfered to qualifier
QUALIFIER
"qualified" calls get transfered to telemarketer
VoIP SERVICES
CALLER ID SPOOFING
TELEPHONE CARRIERS
PSTN
TELEPHONE CARRIERS

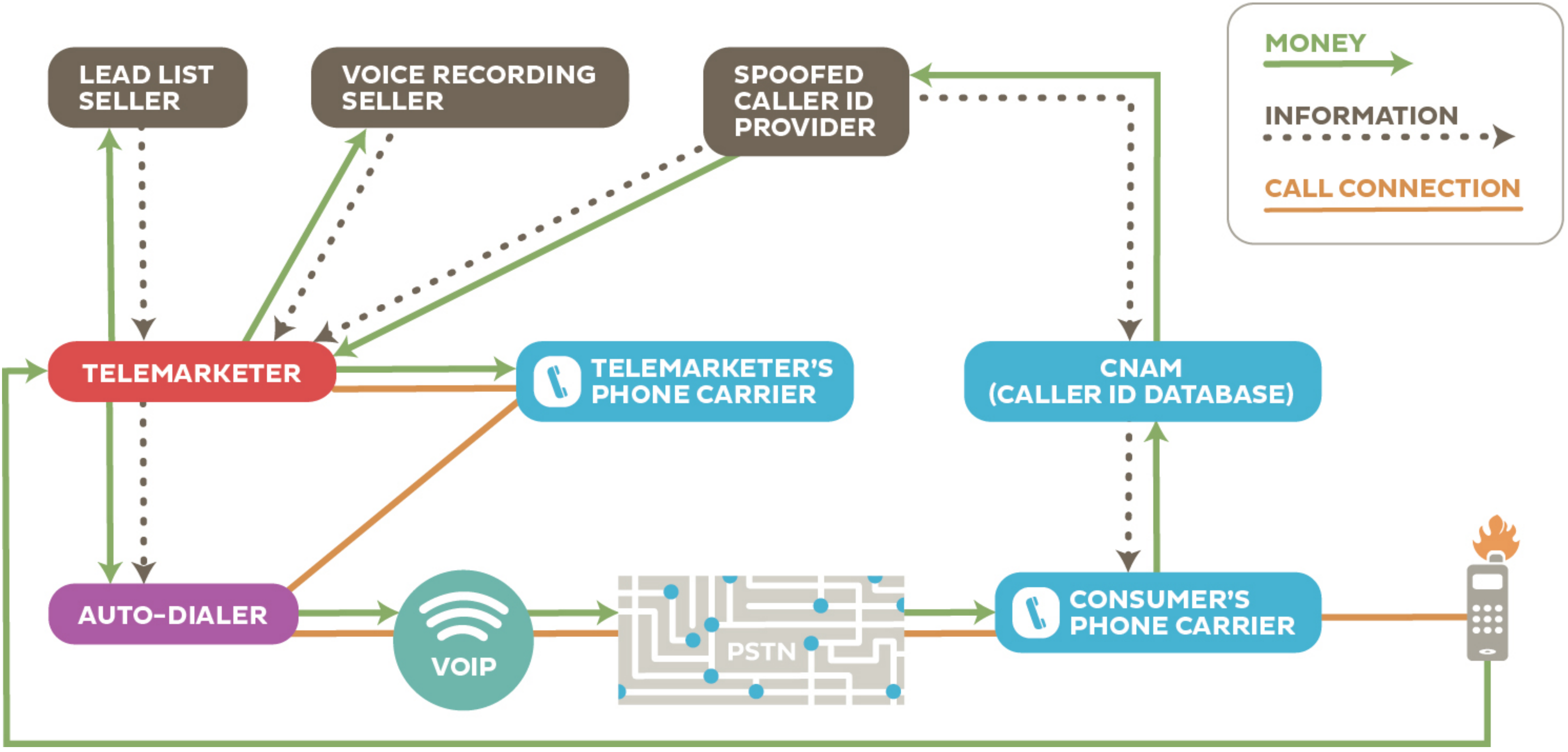
FTC 2012

The geography of robo-calling



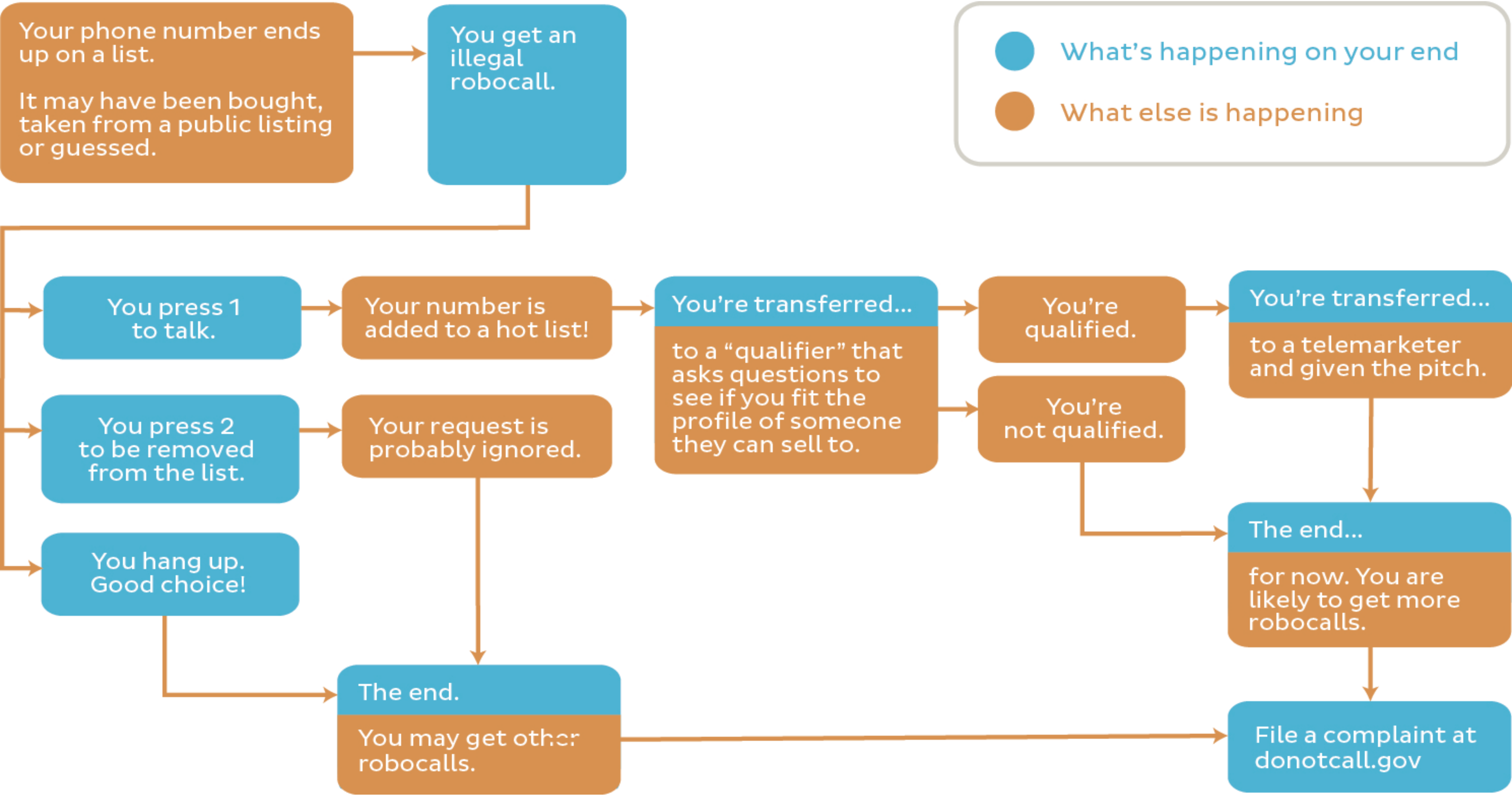
FTC 2012

Robocall eco system



FTC 2012

What you can do when robo-called



● What's happening on your end

● What else is happening

Your phone number ends up on a list.

It may have been bought, taken from a public listing or guessed.

You get an illegal robocall.

You press 1 to talk.

Your number is added to a hot list!

You're transferred... to a "qualifier" that asks questions to see if you fit the profile of someone they can sell to.

You're qualified.

You're transferred... to a telemarketer and given the pitch.

You're not qualified.

The end... for now. You are likely to get more robocalls.

File a complaint at donotcall.gov

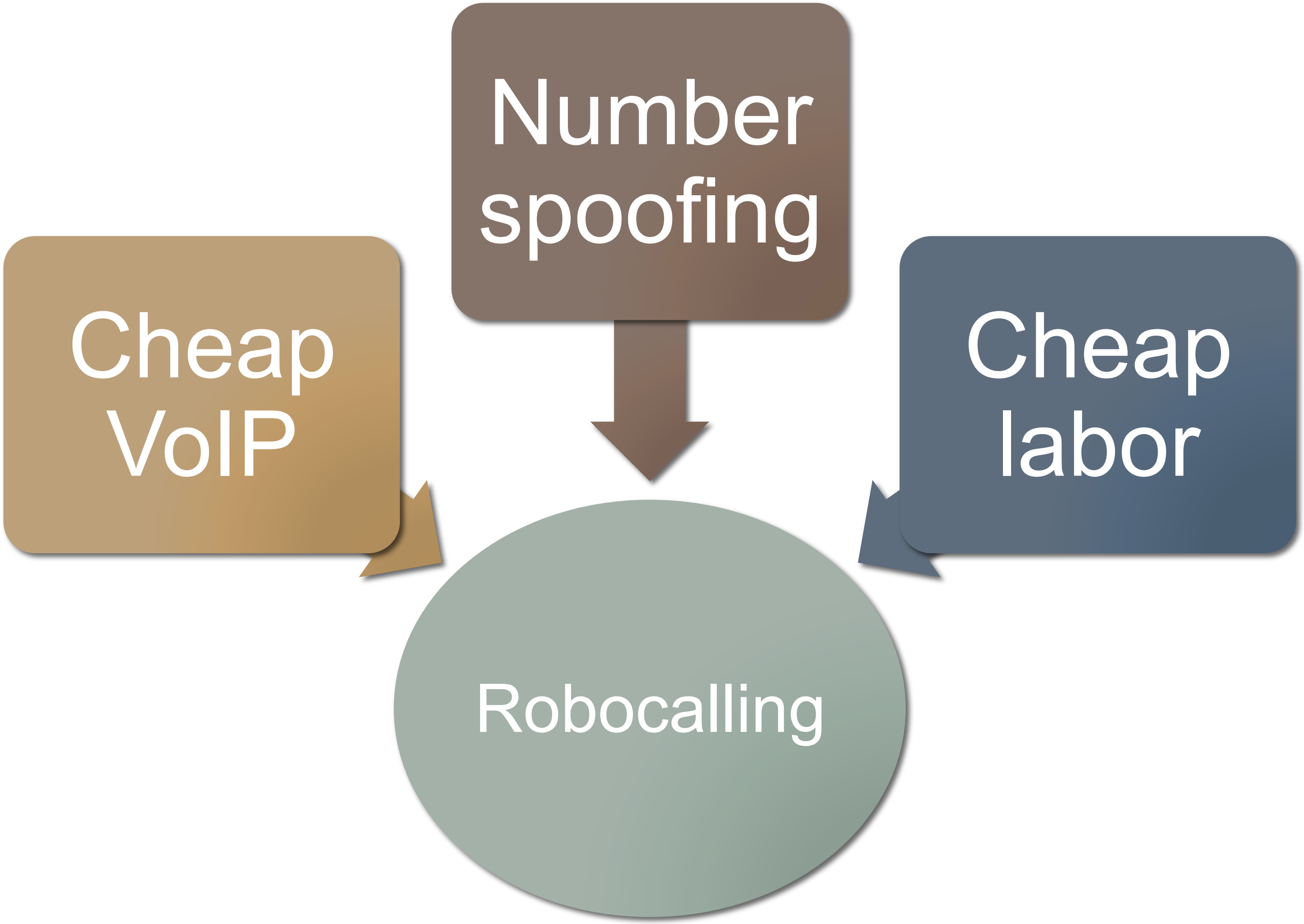
You press 2 to be removed from the list.

Your request is probably ignored.

You hang up. Good choice!

The end. You may get other robocalls.

The enablers



Law enforcement vs. robocallers

- Agile numbering
- Automated customer acquisition
- Transnational

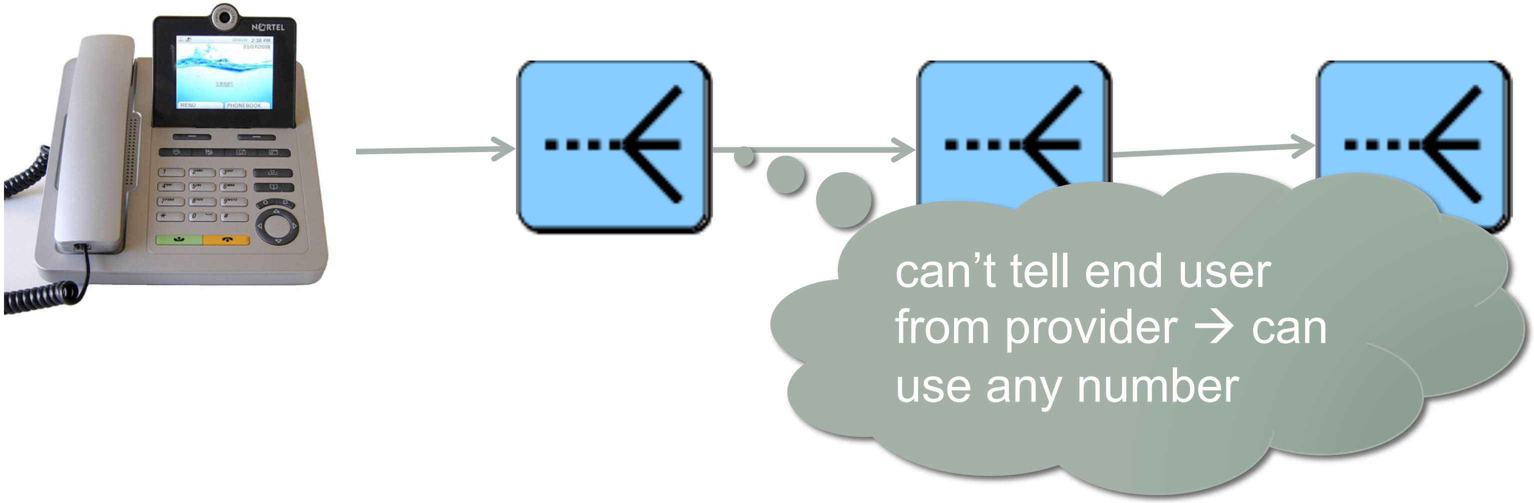
- One faxed subpoena at a time
- Manual trace-back
- Largely domestic

What has changed?

customer

one assigned number

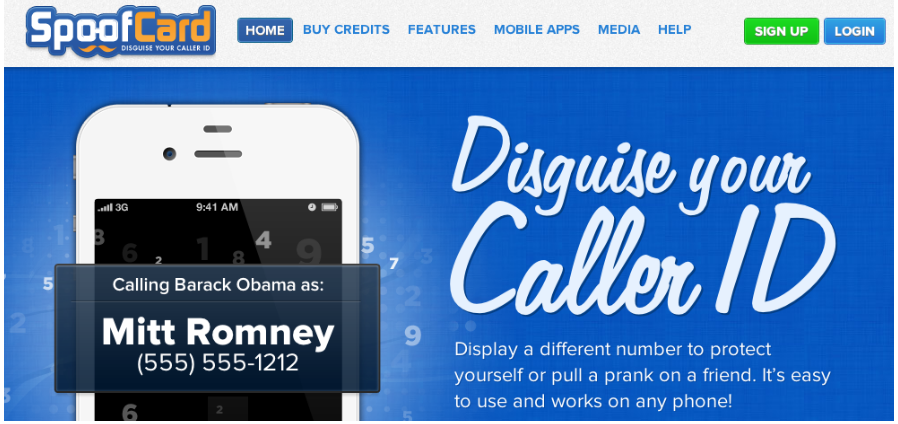
local exchange carrier



can’t tell end user from provider → can use any number

Caller ID spoofing

- Caller ID Act of 2009: *Prohibit any person or entity for transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value.*



Calling Barack Obama as:

Mitt Romney
(555) 555-1212

Disguise your Caller ID

Display a different number to protect yourself or pull a prank on a friend. It's easy to use and works on any phone!

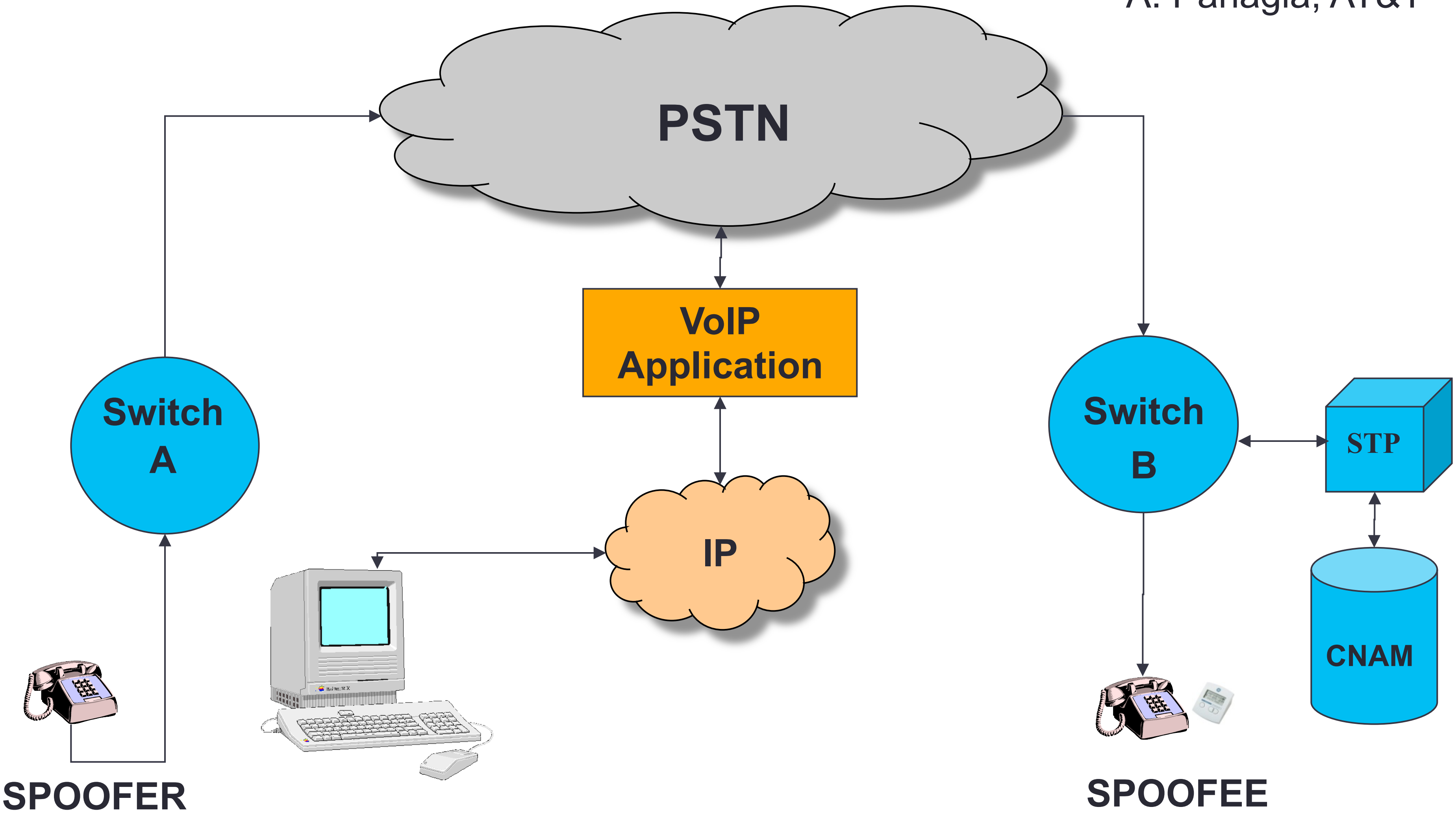
Caller ID spoofing

- enhances theft and sale customer information through pretexting
- harass and intimidate (bomb threats, disconnecting services)
- enables identity theft and theft of services
- compromises and can give access to voice mail boxes
- can result in free calls over toll free dial-around services
- facilitates identification of the name (CNAM) for unlisted numbers
- activate stolen credit cards
- causes incorrect billing because the jurisdiction is incorrect
- impairs assistance to law enforcement in criminal and anti-terrorist investigations

A. Panagia, AT&T

VoIP spoofing

A. Panagia, AT&T



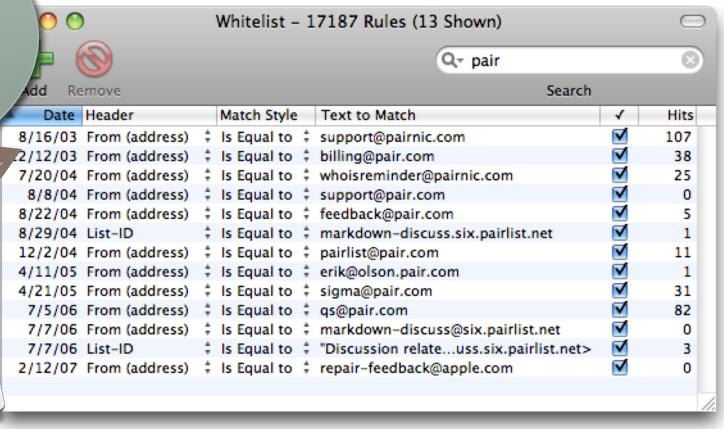
Why not use email spam filtering techniques?

	Email	Phone calls
Name space	infinite	relatively small
Content inspection	common	not possible
Addresses	*IP address* – non-spoofable for TCP *Email address* – easily spoofable	*Phone number* -- spoofable
Delivery	filtered by provider: • block lists (e.g., Spamhaus) • SPF, DKIM	interconnection and delivery obligations
Delivery trace	**Received-by** headers	**Via** headers – only for end-to-end VoIP calls
Limited-use address	easy (e.g., web mail)	not feasible
Consent-based	CAPTCHA systems (not common)	likely too annoying

see also RFC 5039

Future, part 1: trustable phone numbers

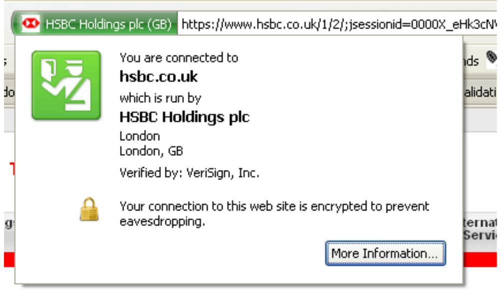
previous contact



Whitelist – 17187 Rules (13 Shown)

pair

Date	Header	Match Style	Text to Match	✓	Hits
8/16/03	From (address)	Is Equal to	support@pairnic.com	☑	107
2/12/03	From (address)	Is Equal to	billing@pair.com	☑	38
7/20/04	From (address)	Is Equal to	whoisreminder@pairnic.com	☑	25
8/8/04	From (address)	Is Equal to	support@pair.com	☑	0
8/22/04	From (address)	Is Equal to	feedback@pair.com	☑	5
8/29/04	List-ID	Is Equal to	markdown-discuss.six.pairlist.net	☑	1
12/2/04	From (address)	Is Equal to	pairlist@pair.com	☑	11
4/11/05	From (address)	Is Equal to	erik@olson.pair.com	☑	1
4/21/05	From (address)	Is Equal to	sigma@pair.com	☑	31
7/5/06	From (address)	Is Equal to	qs@pair.com	☑	82
7/7/06	From (address)	Is Equal to	markdown-discuss@six.pairlist.net	☑	0
7/7/06	List-ID	Is Equal to	"Discussion relate…uss.six.pairlist.net>	☑	3
2/12/07	From (address)	Is Equal to	repair-feedback@apple.com	☑	0



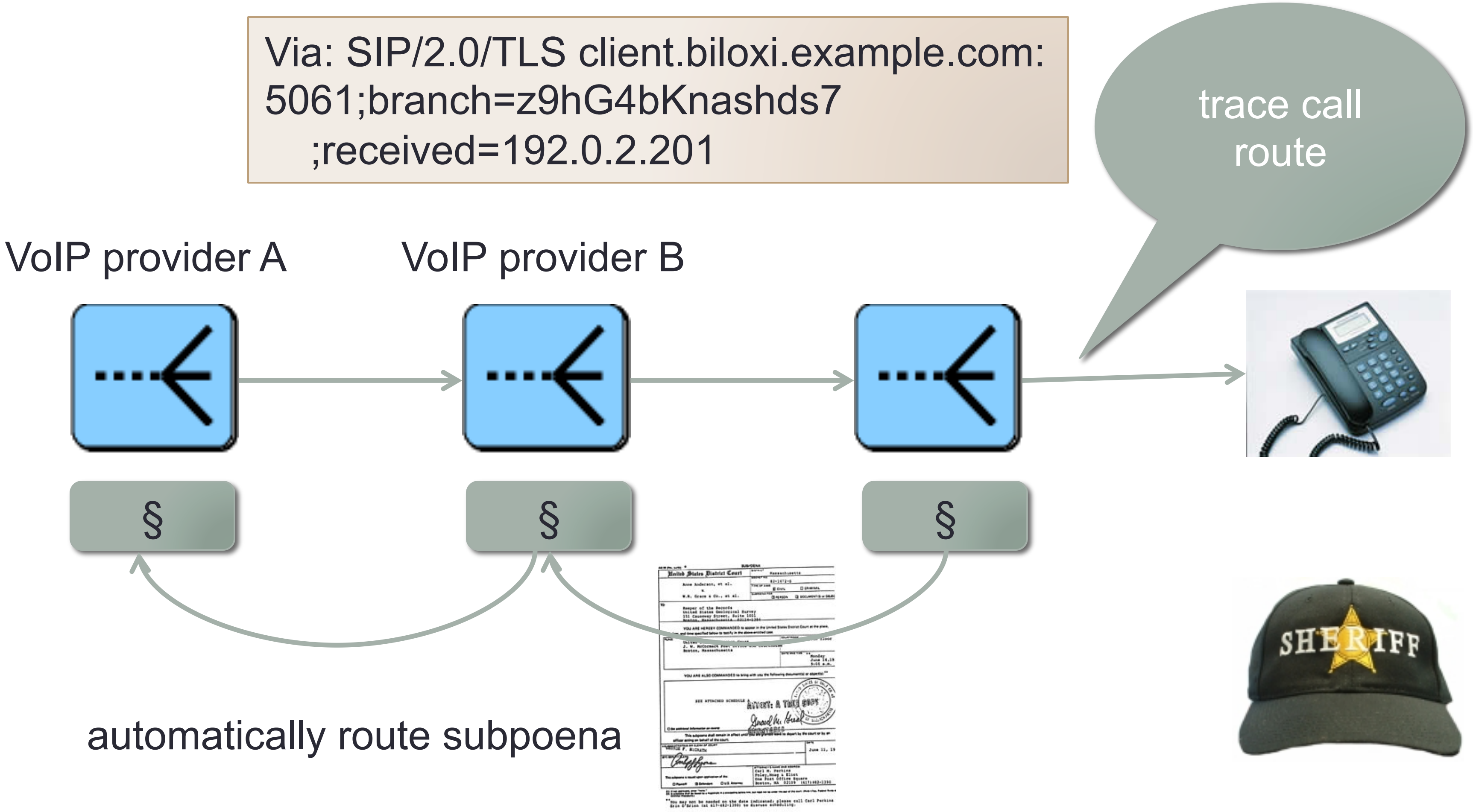
https://www.hsbc.co.uk/1/2/;jsessionid=0000X_eHk3cN

You are connected to
hsbc.co.uk
which is run by
HSBC Holdings plc
London
London, GB

Verified by: VeriSign, Inc.

Your connection to this web site is encrypted to prevent eavesdropping.

IP-based PSTN: build in security!



Via: SIP/2.0/TLS client.biloxi.example.com:
5061;branch=z9hG4bKnashds7
;received=192.0.2.201

automatically route subpoena

SUBPOENA

United States District Court

Massachusetts

82-1672-S

Anne Anderson, et al.
v.
W.R. Grace & Co., et al.

☒ CIVIL ☐ CRIMINAL

☐ PERSON ☐ DOCUMENT(S) or OBJECT(S)

TO:
Keeper of the Records
United States Geological Survey
151 Causeway Street, Suite 1001
Boston, Massachusetts 02114-1384

YOU ARE HEREBY COMMANDED to appear in the United States District Court at the place, date, and time specified below to testify in the above-entitled case.

PLACE
United States [illegible]
J. W. McCormack Post Office and Courthouse
Boston, Massachusetts

Monday
June 16, 19
9:00 a.m.

YOU ARE ALSO COMMANDED to bring with you the following document(s) or object(s):

SEE ATTACHED SCHEDULE A

ATTEST: A TRUE COPY

This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer acting on behalf of the court.

GEORGE F. MCGRATH

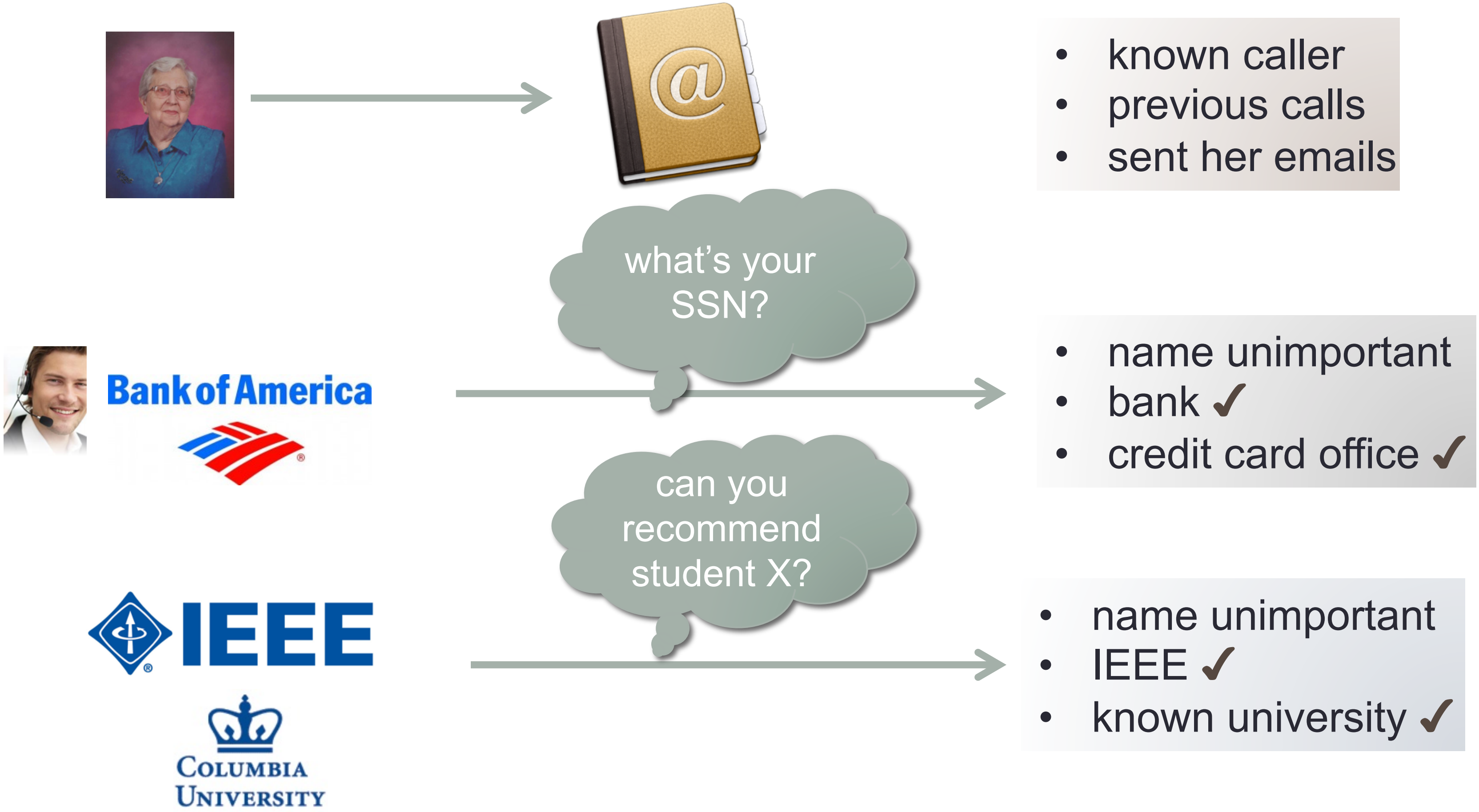
June 11, 19

This subpoena is issued upon application of the:
☐ Plaintiff ☒ Defendant ☐ U.S. Attorney

Carl H. Perkins
Foley, Hoag & Eliot
One Post Office Square
Boston, MA 02109 (617)482-1390

**You may not be needed on the date indicated; please call Carl Perkins
Erin O'Brien (at 617-482-1390) to discuss scheduling.

Caller identification



- known caller
- previous calls
- sent her emails

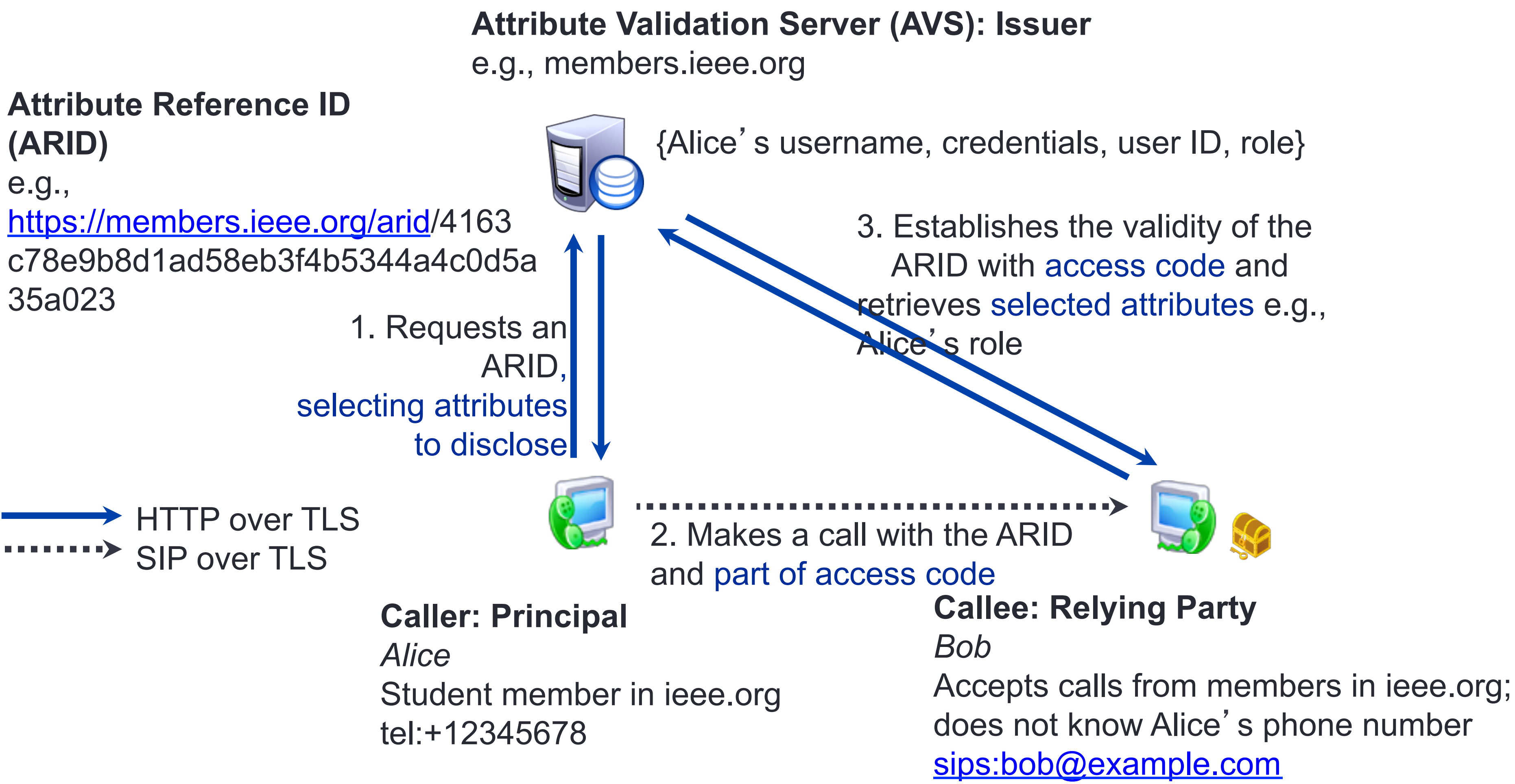
- name unimportant
- bank ✓
- credit card office ✓

- name unimportant
- IEEE ✓
- known university ✓

Attribute validation

- For *unknown* callers, care about attributes, not name
- SIP address-of-record (AOR) → attributes
  - employment (bank, registered 501c3)
  - membership (professional)
  - age (e.g., for mail order of restricted items)
  - geographic location
- Privacy
  - → selective disclosure
  - no need to disclose identity

Attribute Validation Service



Attribute Validation Server (AVS): Issuer
e.g., members.ieee.org

{Alice's username, credentials, user ID, role}

Attribute Reference ID (ARID)
e.g., https://members.ieee.org/arid/4163c78e9b8d1ad58eb3f4b5344a4c0d5a35a023

1. Requests an ARID, selecting attributes to disclose

2. Makes a call with the ARID and part of access code

3. Establishes the validity of the ARID with access code and retrieves selected attributes e.g., Alice's role

HTTP over TLS

SIP over TLS

Caller: Principal
Alice
Student member in ieee.org
tel:+12345678

Callee: Relying Party
Bob
Accepts calls from members in ieee.org; does not know Alice's phone number
sips:bob@example.com