Permissive Action Links and the History of Public Key Cryptography

Steven M. Bellovin

smb@research.att.com

http://www.research.att.com/~smb

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

"Bypassing a PAL should be, as one weapons designer graphically put it, about as complex as performing a tonsillectomy while entering the patient from the wrong end."

What's a PAL, and Why?

- "Permissive Action Link" (originally "Prohibited Action Link")
- The cryptographic combination lock on nuclear weapons.
- Prevents unauthorized use:
  - Enemy countries
  - Terrorists
  - Rogue (or pressured) U.S. troops
  - Our allies.

    ☞The original motivation

Why Are PALs Interesting?

- How do they work? What are the design principles? Supposedly, they cannot be bypassed.
- Is there a lesson more mundane sorts of security mechamisms should emulate?
- The history is interesting, and not fully documented. The original order to deploy PALs (NSAM-160, June 1962) is claimed to be the basis for NSA's invention of public key cryptography in the mid-1960's. What is the relationship?
- I really hope they work as advertised. . .

Disclaimer

- No secrets were stolen in the process of this research
- I’ve never had a clearance
- As far as I know, nothing I’m going to say is classified (even though at one point one reporter and/or the FBI might have suspected otherwise)

The History of PALs

- Envision the 1950s
- The Cold War was in full swing; international relations were *very* tense
- The U.S. was very afraid of a massive Soviet armored invasion of Western Europe. Maintaining a large-enough standing U.S. force in Europe was politically infeasible.
- The answer was simple: NATO, nukes — and NATO members with nukes. . .

Many Kinds of Nukes!

- Strategic weapons, on B-52s and ICBMs (but ICBMs were new and not that reliable)
- Submarine-launched missiles (even newer)
- IRBMs, deployed in various European countries
- Designs for nuclear bomb-powered rockets (Project Orion)
- Nuclear artillery shells
- Nuclear land mines
- Nuclear anti-aircraft missiles
- Nuclear depth charges (the only weapon with a kill probability of 2, if you count the attacking ship)

Who Controlled the Bombs?

- By US law, use of nuclear weapons could only be authorized by the President. (We now know that authority has been delegated to avoid *decapitation attacks*.)
- Did we have adequte control over nuclear weapons stored in various European countries?
- Could we *really* trust our allies?

Attitudes, Not That Long after World War II

We have the missiles, peace to determine,
And one of the fingers on the button will be German.

MLF Lullaby
—Tom Lehrer

Then France got the bomb, but don't you grieve,
'cause they're on our side, I believe!

Who's Next?
—Tom Lehrer

Many Risks

- The Soviets were *extremely* afraid of the Germans
- We didn't fully trust the French
- The Greeks and Turks hated each other

  ☞In 1974, there was apparently a staredown over US nukes between the army and air force of one of those two countries.
- Other danger spots?

Enter PALs

- Strongly opposed by the military
  - Resentment of notion that the (U.S.) military couldn't be trusted
  - Fear that PALs would compromise reliability
- Congressional pressure for more effective U.S. control over European-based weapons
- Eventually, President Kennedy signed National Security Action Memorandum 160, ordering their installation
- The generals were won over by the increased ability to deploy tactical nukes near the front lines without risking Soviet capture — and use — of our bombs

Sometimes, the Risk *Was* the U.S. Military. . .

I used to worry about General Power. I used to worry that General Power was not stable. I used to worry about the fact that he had control over so many weapons and weapon systems and could, under certain conditions, launch the force. Back in the days before we had real positive control [i.e., PAL locks], SAC had the power to do a lot of things, and it was in his hands, and he knew it.

—Gen. Lauris Norstand, deputy commander of SAC, speaking of his boss

Fast Forward 30 Years

- At a Festcolloquium in honor of his retirement from Sandia Labs, Gus Simmons said that he learned of public key crypto the way many of us did, from Martin Gardener's column in *Scientific American*
- 5 minutes later, Jim Frazer – a retired chief cryptographer of NSA — said that NSAM-160 was the basis for NSA's invention of public key cryptography, in the 1960s.
- Simmons agreed with this statement
- Note that this disagrees with the better-documented British claim (which hadn't been declassified at the time)

The Research Project

- Matt Blaze requested NSAM-160 from the Kennedy Library
- ☞ They initiated a declassification request for the memo and for the supporting memorandum
- It arrived mostly intact — and the declassified section had nothing that even hinted at public key crypto...
- Or did it?

In the Middle of a Redacted Section

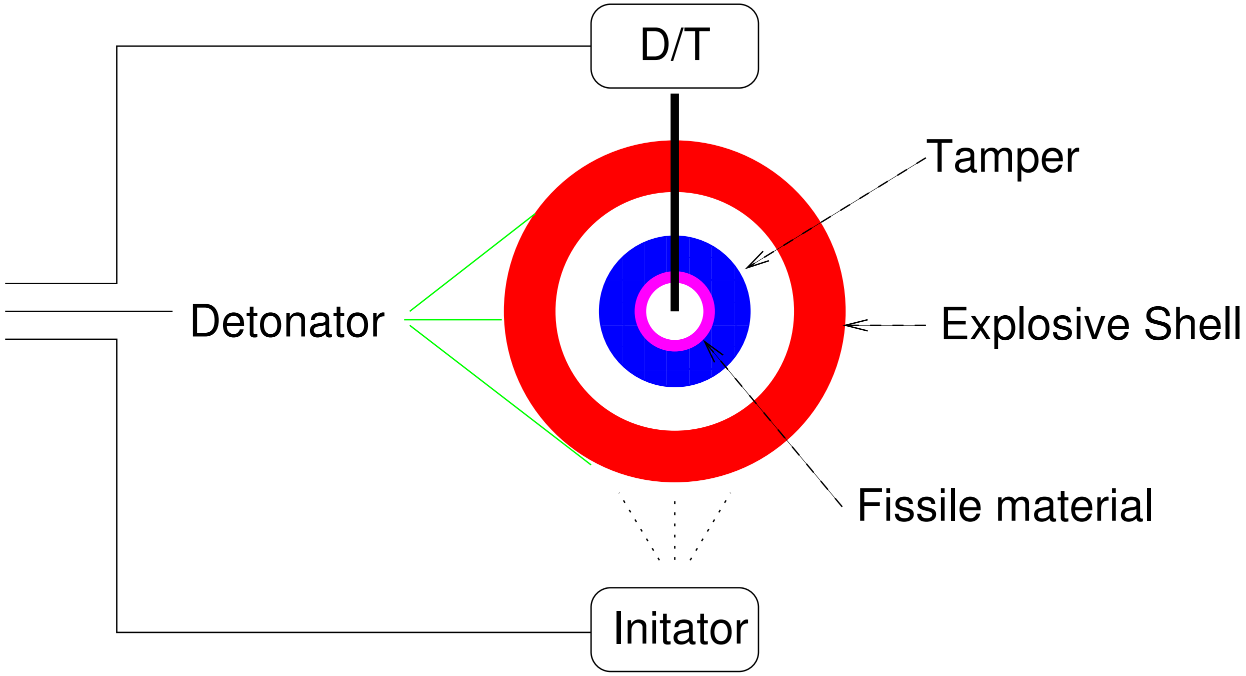
. . . Despite the limitations of this eqiupment, I believe it would give further (and probably decisive) protection against individual psychotics and *would certainly deter unauthorized use by military forces holding the weapons during periods of high tension or military combat. . . .* [emphasis added]

Did this lead to the discovery of digital signatures, and hence non-repudiation?

More Research

- Lots of library work
- (My small, suburban library was able to get all sorts of unusual things via inter-library loan.)
- Not all that much information online
- Technical publications from Sandia Labs
- Freedom of Information Act requests
  ☞They arrive “redacted”
- Nothing conclusive — but I learned a lot about nuclear weapons command and control
- I needed to understand how bombs worked, in order to understand how they could be protected

How Bombs Work

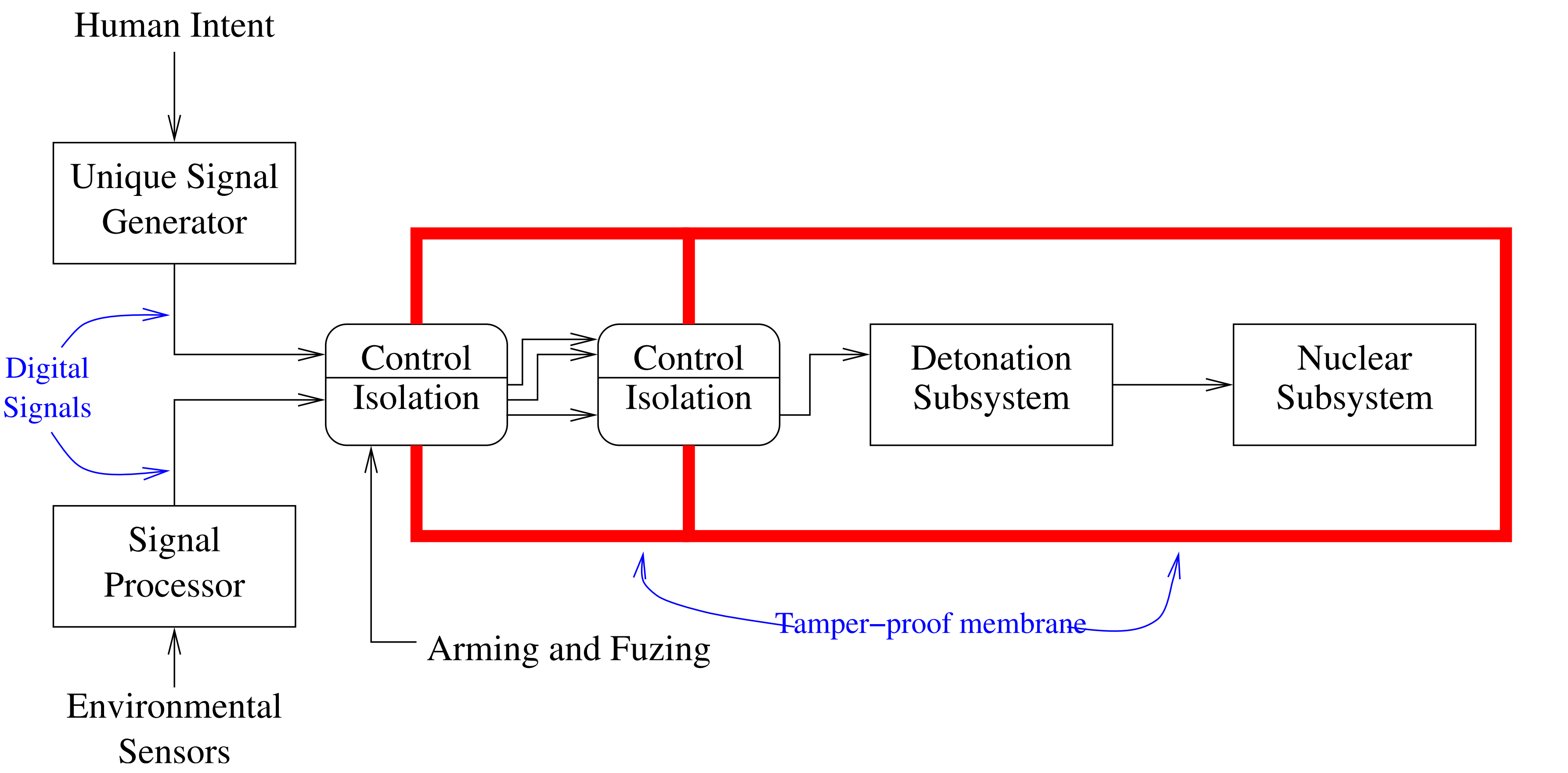


The deuterium/tritium pump, the initiator (the initial neutron source), and the detonators are all controlled by the sequencer. The first two require high voltage sources. Timing is critical to yield.

Safety Features

- One-point safety – no nuclear yield from detonation of one explosive charge.
- Strong link/weak link – strong link provides electrical isolation; weak link fails early under stress (heat, etc.)
- Environmental sensors – detect flight trajectory.
- Unique signal generator – digital signal used for coupling between stages.
- Insulation of the detonators from electrical energy.
- “Human intent” input.
- Tamper-resistant skin.
- Use control systems.

Bomb Safety Systems



Unique Signal Generator

- Part of the strong link
- Prevent any detonation without clear, unambiguous showing of "human intent"
- A *safety* system, not a *security* system
- Looks for 24-bit signal that is *extremely* unlikely to happen during any conceivable accident. (Format of input bits not safety-critical)
- ☞ Accidents can generate random or non-random data streams
- ☞ Desired signal pattern is unclassified!
- Unique signal discriminator locks up on a single erroneous bit
- At least partially mechanical
- Sample conclusion: keyboards not suitable input device

PALs

- Originally electromechanical. (Some weapons used combination locks.)
- Newest model is microprocessor-based. There may still be a mechanical component.
- Recent PAL codes are 6 or 12 digits.
- The weapon will permanently disable itself if too many wrong codes are entered.
- PALs respond to a variety of codes – several different arming codes for different groups of weapons, disarm, test, rekey, etc.
- It was possible, though difficult, to bypass early PALs. (Some even used false markings to deceive folks who didn't have the manual.) It does not appear to be possible to bypass the newest "CAT F" PAL.

Possible Design Principles

- Encrypted timing information.
- High voltage source interruption.
- Encrypted signal paths.
- Encrypted code

Encrypted Timing Information

Can you encrypt the detonation sequence timing information, and fire different explosives at different times?

- Getting a symmetric shock wave is hard enough as is. So is finding suitable explosives.
- There is no published evidence to support this hypothesis. For spherical “pits”, it would seem to be very difficult to do.
- Modern high-efficiency bombs use just two-point detonation — not a lot of variables to play with.
- There would still be the risk of serious U-235 or Pu-239 contamination.
- Control of the D/T reservoir and the initiator *is* feasible – but the former affects only the yield, and for the latter, there is still a non-negligible probability of detonation in the absence of external neutron injection.

High Voltage Source Interruption

- Safety systems rely on keeping electrical energy away from the detonators.
- Several sources hint that PALs work in the same way, by controlling one of the “strong links”.
- Encrypting the environmental sensor signal path is almost free in this design.
- Query: can encrypted timing information be used to prevent charging of the high-voltage capacitors? Probably not.

Hypothesized Design 1

- PALs use several switches to control the high voltage path to the detonators.
- The original designs used rotors similar to those on World War II-vintage encryption machines. The technology was simple, reliable, and well-understood in 1962.
- Newer ones use a a microprocessor to control the switches. This may work by providing a encryption key for the environmental sensors; the signal is decrypted by the strong links.
- The tamper-resistant skin prevents bypass attempts.

Hypothesized Design 2

- If there's a microprocessor inside, it's because the internal control and sequencing requirments are complex
- This timing information, or even the actual code paths, are encrypted
- The public external interface would handle training keys, resets, key changes, etc. — plus, of course, decrypting the sensitive parts
- High assurance — *if* the sequencing really has to be that complex

Security Criteria

- Reading the safety literature (i.e., on strong links) shows a major focus on self-contained mechanisms: Detailed analysis of *one* module's properties, which can do its job independent of most other decision decisions.

☞ Familiar to computer security geeks — we call it a TCB

- The vital secret isn't within the module — an attacker can't reverse-engineer a device to learn how to arm it
- It must interrupt a very vital path that is common to all nuclear weapons of the appropriate class

Is a PAL Like a Unique Signal Discriminator?

- Some evidence that they use the same two-input principle as UQS units
- Similar evidence of the lock-up principle
- Well studied properties
- Reuse some of the idea?

Where's the Cryptography?

- I have found no requirement for the use of public key cryptography in the PALs, nor any hint that it's used there.
- The short PAL sequences make it improbable in any event; no known public key cryptosystem is secure with such short keys.
- PAL codes are moderately widely distributed, albeit in encrypted form.
- A prototype public key PAL was built — but not deployed — in the late 1980s.
- There are many cryptographic tricks to permit shared control schemes.
- Hypothesis: the requirement for authentication of the arming code led NSA to invent digital signatures – which were not invented by the British in the early 1970's.

Maybe it's Cryptographic Engineering

- How does the key get into the PAL?
- Alternatively, if the PAL generates its own key, how is it exported to *only* the right place?
- Passing keys in the clear is very much against NSA practice
- One solution involves public key crypto; is that where the requirement came from?

Command, Control, and the Football

- The President's authorization codes are on a small card he carries with him. (Carter's codes were once sent to the cleaners; the FBI accidentally took Reagan's after he was shot.)
- The detailed attack messages are in the "football" — but these contains authorization codes, not PAL codes.)
- Encrypted PAL codes are deployed at air force bases
- The *authorization* messages – from the President or his appointees – are longer, and could be digitally signed and contain the key to decrypt the PAL codes.
- But — ELF messages to submerged subs are sent at 1 bit/*minute*

Deployment of PALs

- Despite Kennedy's order, PALs were not deployed that quickly.
- ☞ In 1974, there were still some unprotected nukes in Greece or Turkey
- PALs and use control systems were deployed on US-based strategic missiles by then — but the launch code was set to 00000000
- A use control system was added to submarine-based missiles by 1997
- In 1981, half of the PALs were still mechanical combination locks

Who Has PALs?

- In 1971, the US offered the technology to the Soviets.
- They declined, preferring “people watching people who watched still other people”.
  ☞The Soviets used three-party control: the military, the KGB, and a political officer
- What about the rumored Soviet “suitcase bombs”?
- There’s more worry about rogue users within a country than the country itself. Did we offer the technology to France? China? (They asked for the technology in the 1990s.) Israel? India? Pakistan?

Conclusions

- I still don't know anything definite on how PALs work (but I did learn a lot of other things, many of them directly relevant to my day job)
- It's unclear if the issue really did lead to public key cryptography
- But — the British invented public key *encryption*; did the NSA invent *digital signatures*?
- I haven't yet found anything about setting C.R.M.-114 discriminators to ”FGD 135”, let alone ”OPE”. . .

Lesson for Computer Security Geeks

- Understand what problem you're solving
- Understand *exactly* what problem you're solving
- If your abstraction is right, you can solve the key piece of the overall puzzle
- For access control, find the One True Mandatory Path — and block it.
- What is the *real* TCB of our systems?

References

NSAM 160 `http://www.research.att.com/~smb/nsam-160`

PALs

`http://www.research.att.com/~smb/nsam-160/pal.html`