

CodeSeal Overview

Adrian Chavez

adrchav@sandia.gov

(505)284-6664

Network Assurance and Survivability

Craig Smith

casmith@sandia.gov

(925)294-3358

Technology Commercialization

John Solis

jhsolis@sandia.gov

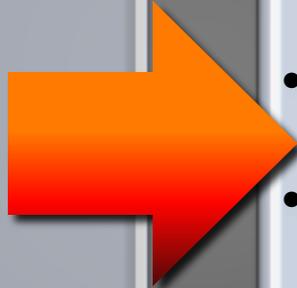
(925)294-2290

Scalable and Secure Systems Research

Your Environment is Compromised – We Have a Solution

Best Practices

- Open specifications
- Assume a clean system to start
- Install security services
- Perform regular maintenance
- Hire dedicated security staff
- Protect subsystems based on organizational roles



Sophisticated Adversaries

- Exploit design details
- Influence the supply chain
- Exploit security services
- Provide maintenance services
- Hire your dedicated security staff
- Act according to the goal, disregarding arbitrary boundaries



Financial Losses ARE REAL

- July 2013: U.S. federal prosecutors file charges against **five** Russian hackers*
 - 160 million credit and debit card numbers from 16 separate corporate victims
 - 2006: PNC Bank's online site attacked - **\$1.3 million**
 - 2007: Citibank ATMs – 100k customers - **\$2.9 million**
 - 2008: Citibank online banking – 300k customers - **\$3.6m**
- May 2013: **Seven** masterminds arrested in UAE
 - 40k ATM withdrawals in 27 countries - **\$45 million**
- Banking/finance industry attacked **once every six minutes****

Sources: * <http://spectrum.ieee.org/riskfactor/telecom/security/this-week-in-cybercrime-online-bank-heists-just-the-latest-in-a-long-string>

**<http://www2.fireeye.com/rs/fireeye/images/fireeye-advanced-threat-report-2h2012.pdf>



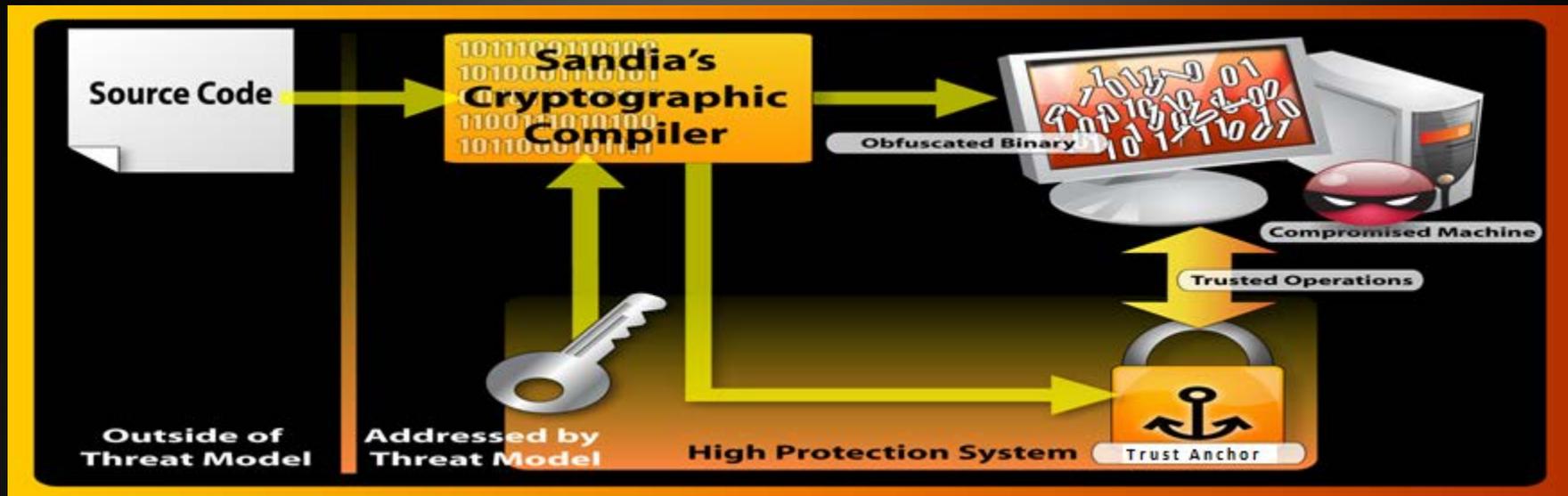
Sandia
National
Laboratories

Need

- Protect credit card (CC) payment processing systems
 - Heartland Payment Systems Inc – 130 million CCs
 - Commidea Ltd – European payment processor – 30 million CCs
 - Euronet (Leawood, Kansas) – 2 million CCs to malware
- Trusted Execution in Untrusted Environments
 - Certainty that payment processing operations cannot be tampered with
 - Make security functions undetectable to malware
 - Realize benefits of COTS while reducing risk



Approach: Trust Anchors as a Basis of New Security Services

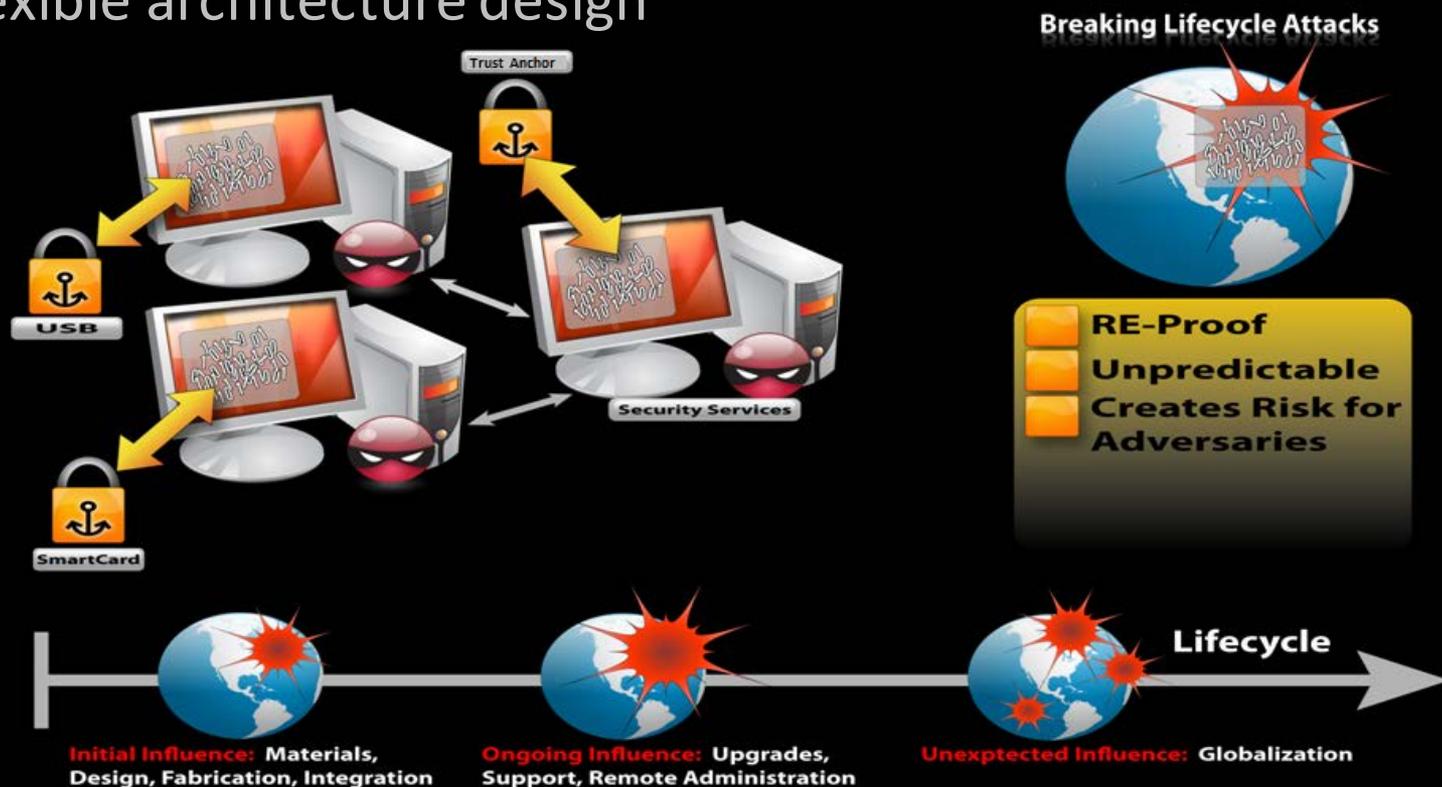


- Foundation for reliable security services that cannot be maliciously influenced
- Security functions undetectable to malware
- Tampering of protected code is detected



Benefits

- Provably secure cryptographic strength
- Anti-reverse engineering / Integrity of execution
- Flexible architecture design



Competition

- Traditional obfuscation
 - Can be reverse engineered
 - Assumes adversary cannot analyze our systems
- Vulnerability assessments
 - Expensive (\$500K/assessment) and time consuming (1-12 months)
 - Detection can still be elusive



Next Steps

- Collaborate with partners on high exposure systems for a focused pilot deployment
- Upcoming Testing & Evaluation
 - Need **real-world** use-case
 - Let us test yours!
- Iterative collaboration to tailor technology to specific environments



Publications

- “On the Secure Obfuscation of Deterministic Finite Automata”, W. Erik Anderson, <http://eprint.iacr.org/2008/184.pdf>
- “Position Paper: Protecting Process Control Systems against Lifecycle Attacks Using Trust Anchors”, Adrian R Chavez, <http://cimic.rutgers.edu/positionPapers/DHSPositionPaperAdrianChavez.pdf>

CodeSeal Contact Info

Adrian Chavez

adrchav@sandia.gov

(505)284-6664

Network Assurance and Survivability

Craig Smith

casmith@sandia.gov

(925)294-3358

Technology Commercialization

John Solis

jhsolis@sandia.gov

(925)294-2290

Scalable and Secure Systems Research



Sandia
National
Laboratories