Cryptosense

Crypto Risk

GRAHAM STEEL

November 2016

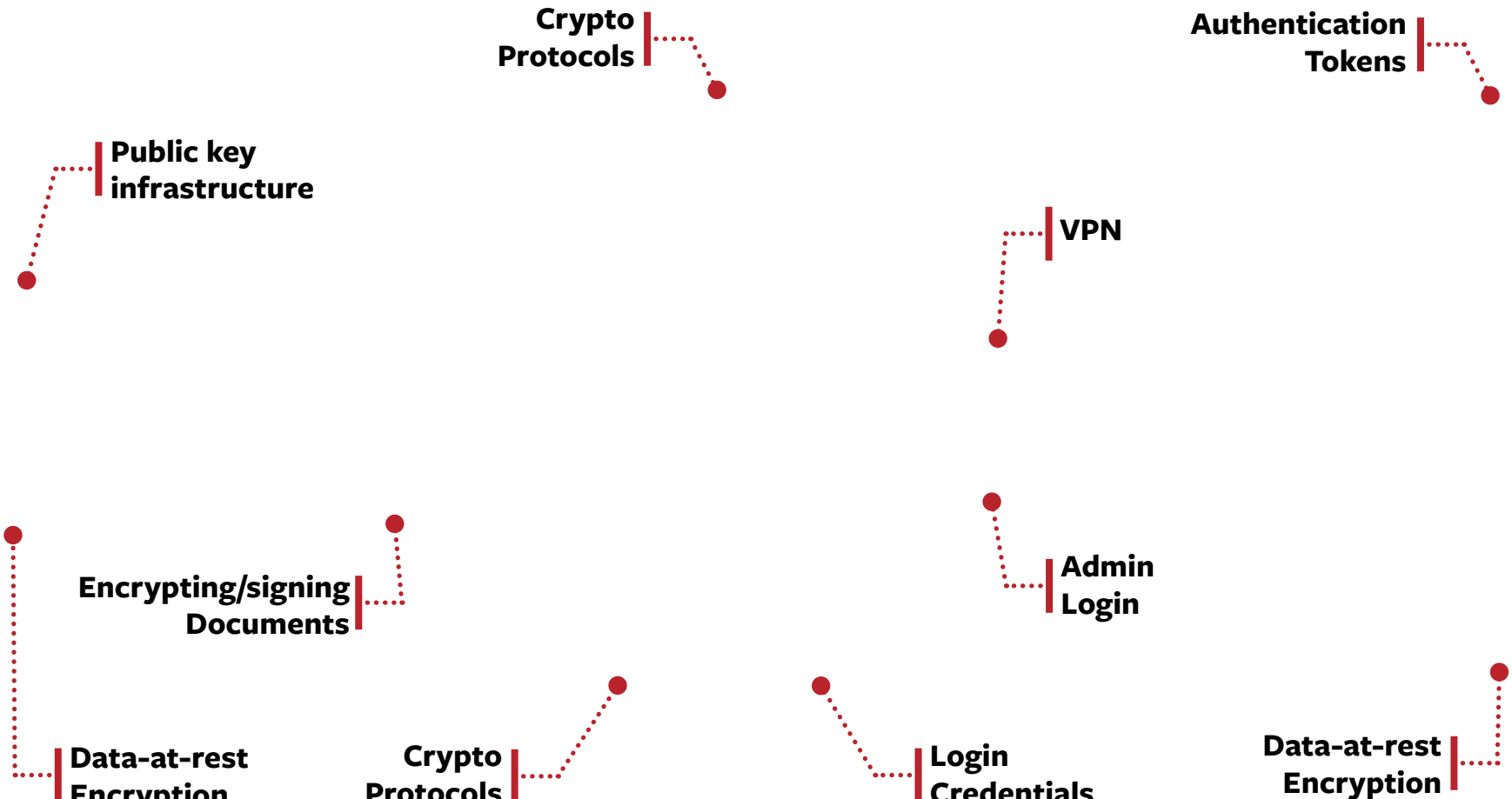
What is ‘crypto risk’?

Cryptography is the cornerstone of security in modern IT infrastructure, including IoT.

Crypto risk is the danger of suffering harm or loss if crypto doesn’t work as it should.

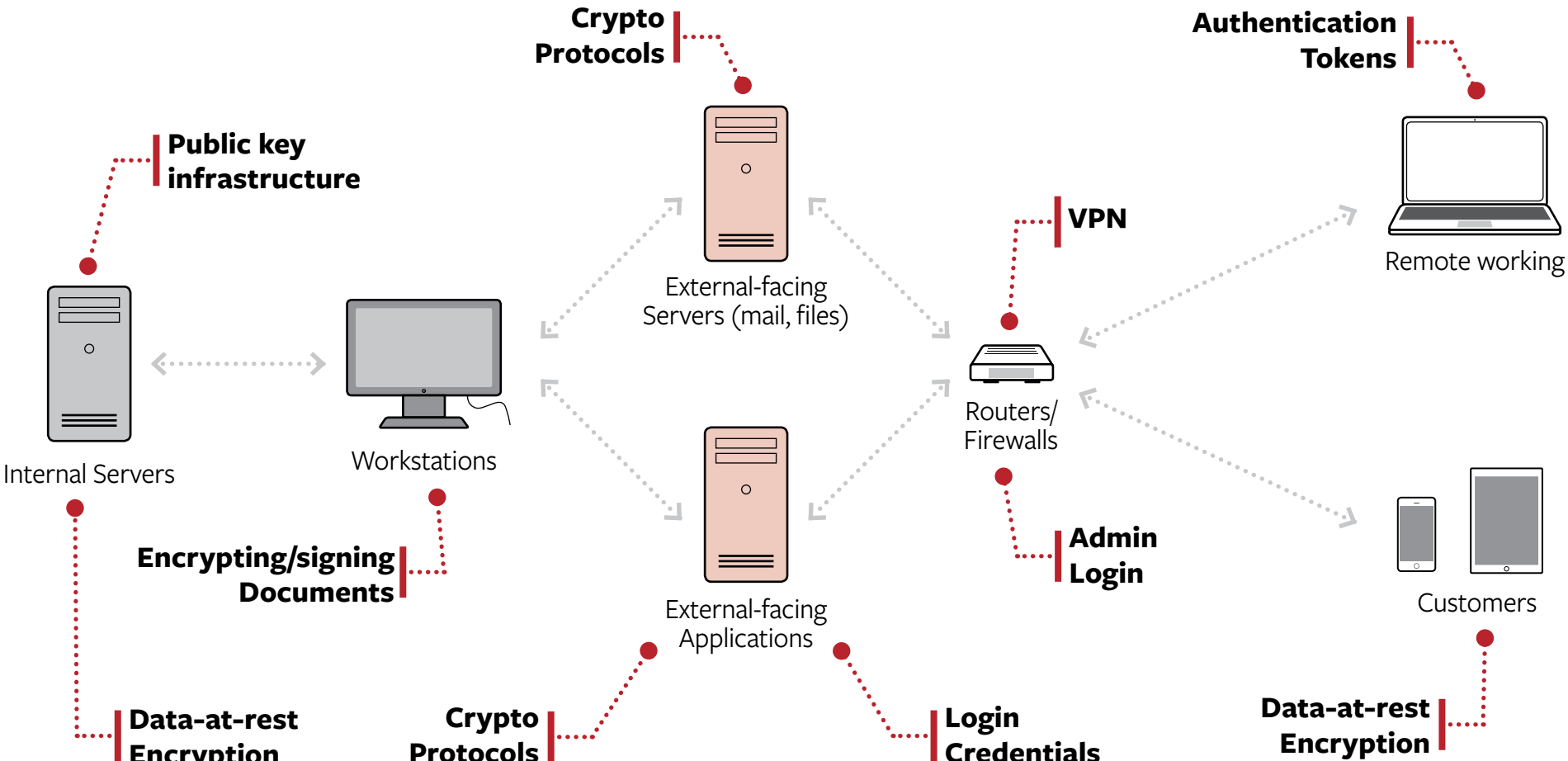
“We don’t use cryptography”

“We don’t use cryptography”



Cryptosense

“We don’t use cryptography”



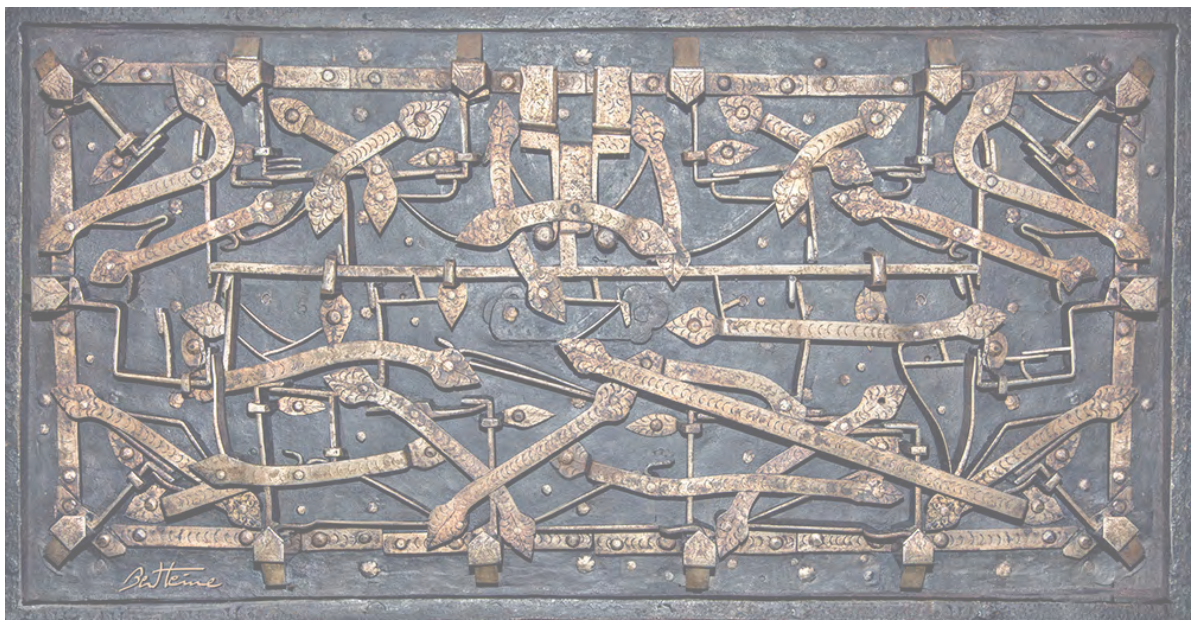
Are crypto attacks really a threat?

Previously the domain of state-level actors only, attacking weak or poorly-used crypto is now a standard hacker skill.

- 3 trainings on attacking crypto, 6 talks on new crypto attacks at Black Hat/DEFCON 2016
- 6 major widely-applicable crypto attacks in academic conferences in 2015 (FREAK, LOGJAM, Off-curve attacks..)
- Matasano crypto challenges (cryptopals.org) walk through dozens of examples.

People think that crypto looks like this.

...but it's really more like this.



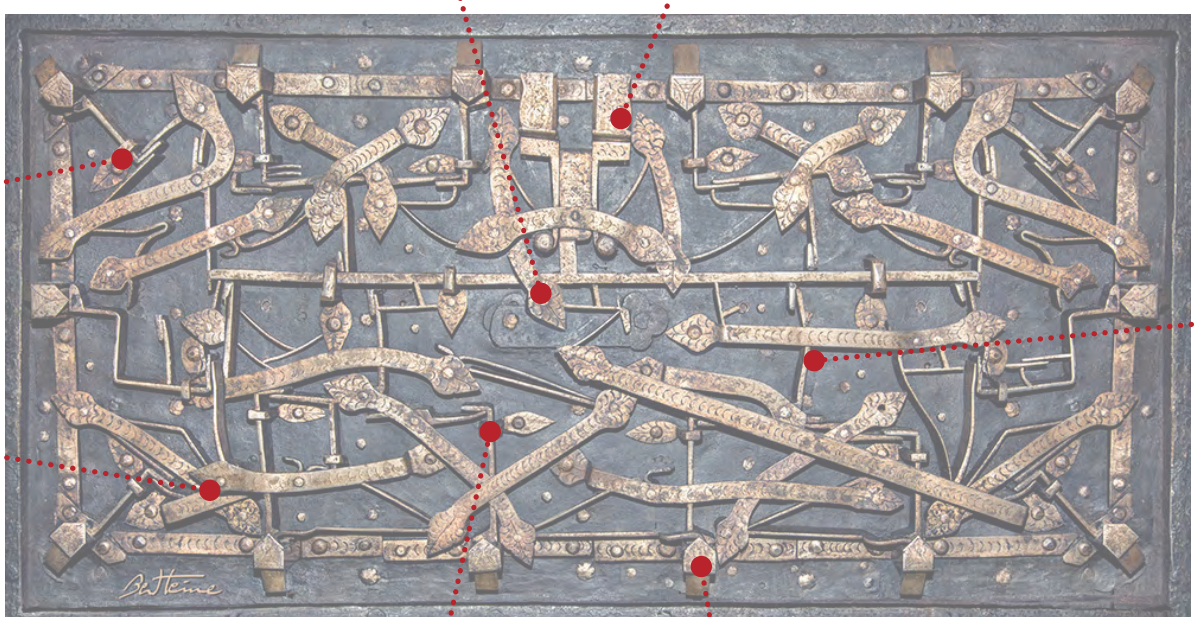
16th Century, Citadel of Dinant, Belgium.

Photo © *2016* *Ben Heine*

Problems with random number generation

Interactions between crypto operations

Key-management flaws



Protocol configuration errors

Bad nonce management

Weak encryption and signature modes

Weak algorithm and key-length choice

Photo © 2016 Ben Heine

Problems with random number generation

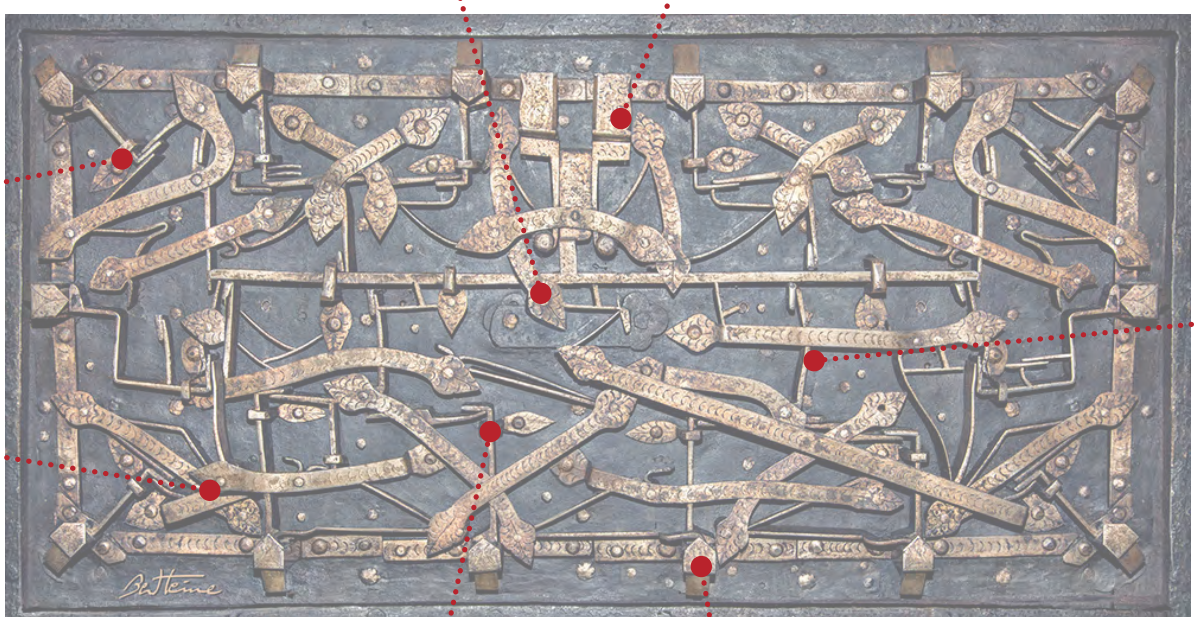
RSA keys GCD
January 2012

Interactions between crypto operations

RBS Worldpay heist
November 2008

Key-management flaws

RSA SecurID seed
March 2011



Protocol configuration errors

DROWN
March 2016

Bad nonce management

Sony Playstation
December 2010

Weak encryption and signature modes

PKCS#1v1.5 signature
January 2016

Weak algorithm and key-length choice

FLAME
May 2012

This talk will cover each of these incidents and explain:

- What went wrong
- What were the consequences
- Where else the same problem can be found
- How to detect and avoid the problem in the future

Key Management

- Creation
- Destruction
- Distribution
- Storage
- Use
- Backup, restore, refresh...

"Key management is the hardest part of cryptography and often the Achilles' heel of an otherwise secure system."

B. Schneier, Applied Cryptography (2nd edition)

Key Management | RSA SecurID Breach

Announced March 2011

- Seed values for devices stored insecurely, compromised after phishing breach.
- 40M devices replaced, Lockheed-Martin breached, massive brand damage.

Other examples: weak key storage on disk, poorly configured HSMs...

Random Number Generation

Vital for cryptography.

- Key generation
- Blinding
- Salt values
- Challenges
- IVs
- Padding...

"Random number generation is too important to be left to chance."

Robert Coveyou

Random Number Generation | Batch-GCD attacks on RSA key generation

January 2012

More than 20,000 TLS and SSH keys broken.

Data Set	Date	Total Unique Moduli	Factored Unique Moduli
Lenstra et al. (PGP + X.509 Certificates)	11/2011	6,386,984	12,934 (0.20%)
Heninger et al. (TLS)	10/2011	5,656,519	23,576 (0.42%)
Heninger et al. (SSH)	02/2012	3,821,639	1,013 (0.027%)
Cryptosense (TLS)	07/2015	13,609,008	19,126 (0.14%)
Cryptosense (SSH)	04/2016	7,725,893	677 (0.009%)

Also found: blacklisted keys, backdoors, faulty embedded devices.

Encryption and Signature Modes

In order to apply them to data, cryptographic algorithms must be combined with ‘modes’ that specify padding, chaining of blocks, etc.

Using the wrong mode can result in insecurity even if the algorithm is perfectly secure.

Encryption and Signature Modes | RSA PKCS#1v1.5 Signature Forgery

- Superceded in 2003 by RSA PSS, but slow uptake.
- Attack revealed by **Bleichenbacher 2006**.
- Found in OpenSSL, Java, NSS, GNUTLS.
- **January 2016** found by Valsorda in python crypto library (>100k daily downloads)

Also found: ECB mode, PKCS#1v1.5 encryption, CBC without authentication...

Nonce Management

A nonce is a value that is only used once - it is not necessarily unpredictable.

Once-only property is vital: many cryptographic operations fail catastrophically if a value is used twice.

Nonce Management | Sony Playstation

ECDSA flaw Dec 2010

- Reuse of nonces in ECDSA signature mode led to loss of private key.
- DRM completely broken.

Also found: Nonce reuse on TLS servers

Protocol Configuration Errors

SSH, TLS, IPSec, etc. have rich configuration options

Many are insecure, and the game is always changing (FREAK, BEAST, CRIME, LOGJAM, etc.)

Challenge is to decide the right policy and monitor and enforce it everywhere.

Protocol Configuration Errors | DROWN

Announced March 1st 2016, 33% of HTTPS sites affected

- Practical SSLv2 attack
- Many servers left SSLv2 on "just in case" as all modern browsers refuse it anyway.
- SSLV2 connection could be used to break TLSv1.2

Also found: Old SSL in embedded devices, legacy Java applications.

Interaction between Crypto Operations

Operation **A** is secure.

Operation **B** is secure.

But Operation **A** followed by Operation **B** breaks security completely.

Interaction between Crypto Operations | RBS Worldpay Heist

November 2008 - $9.4M ATM fraud

- HSM was left with too many PIN processing commands enabled
- Allowed attackers to build codebook and crack PINs

Also found: Encrypt and MAC, Sign and Decrypt.

Weak Algorithms

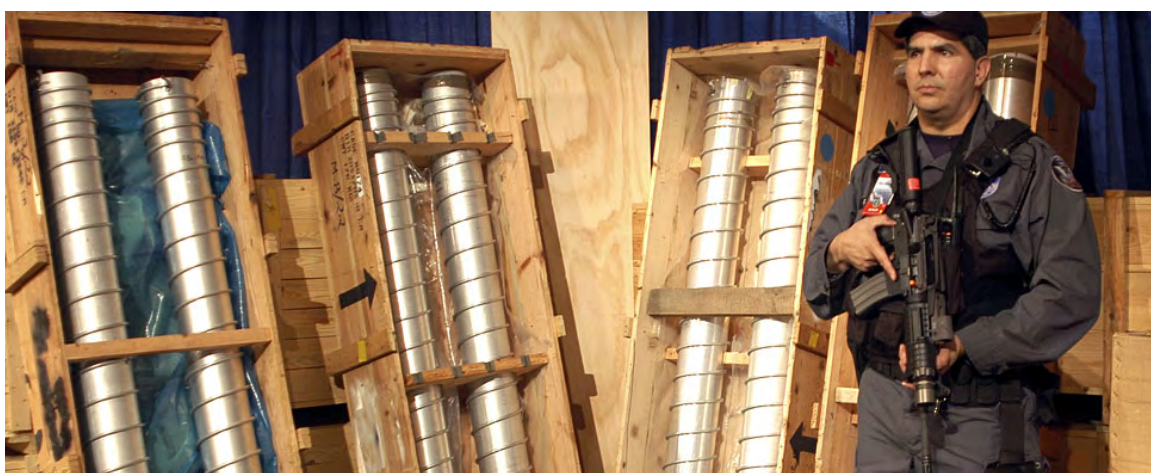
Many are well known, however the state of the art is always changing.

Weak algorithms are often hidden inside libraries and application frameworks.

Weak Algorithms | FLAME

May 2012, sophisticated attack on Iranian nuclear programme

- To bypass code update check, a fake certificate using an MD5 collision was used.
- MD5 Collision method used was different from that publicly known.



Also found: Single DES, SHA-1 certificates

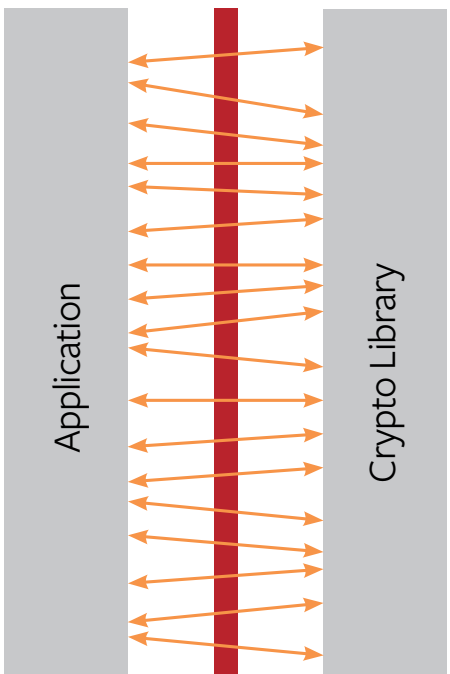
1806 crypto misuse vulnerabilities added to the Mitre CVE database 2013 - 2015

83% of crypto bugs are in **applications**, not in cryptographic library code*

98.3% of crypto flaws **cannot be detected** by the best performing static analysis tool**

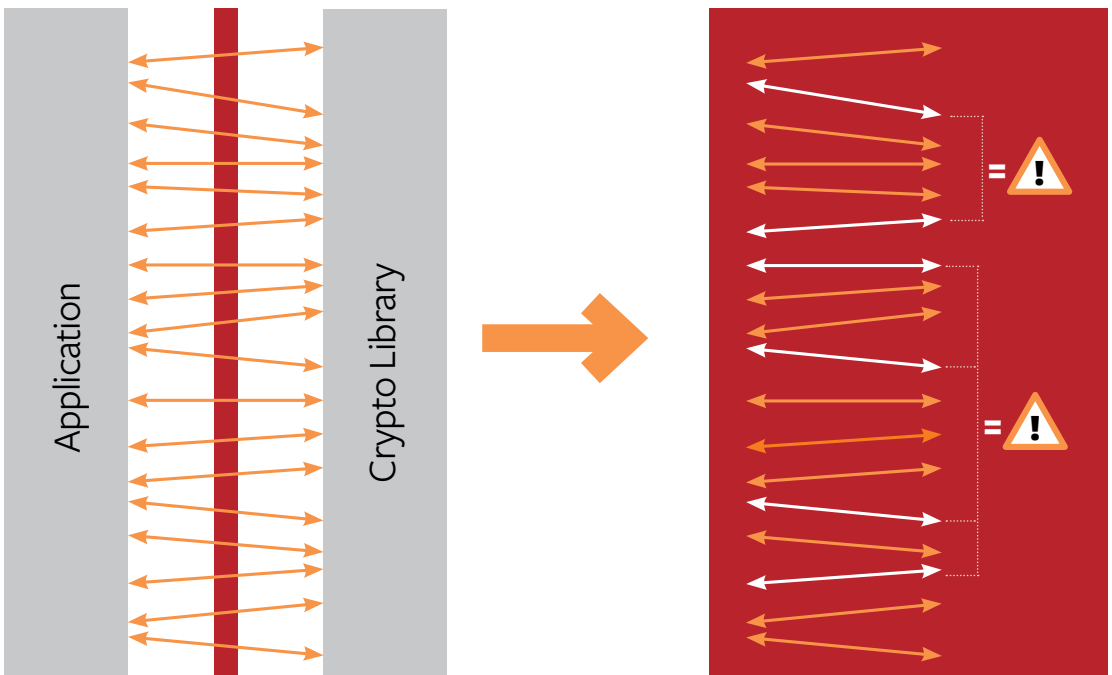
** Lazar et al, Why does Cryptographic software fail? APSys '14*
*** 2013 NIST SATE Evaluation*

Cryptosense software **attaches to a running application** or network service on the customer's infrastructure and logs crypto calls.



1. Tracing

Traces are run through our **security analysis algorithms** derived from the latest academic results and Cryptosense's own vulnerability research.

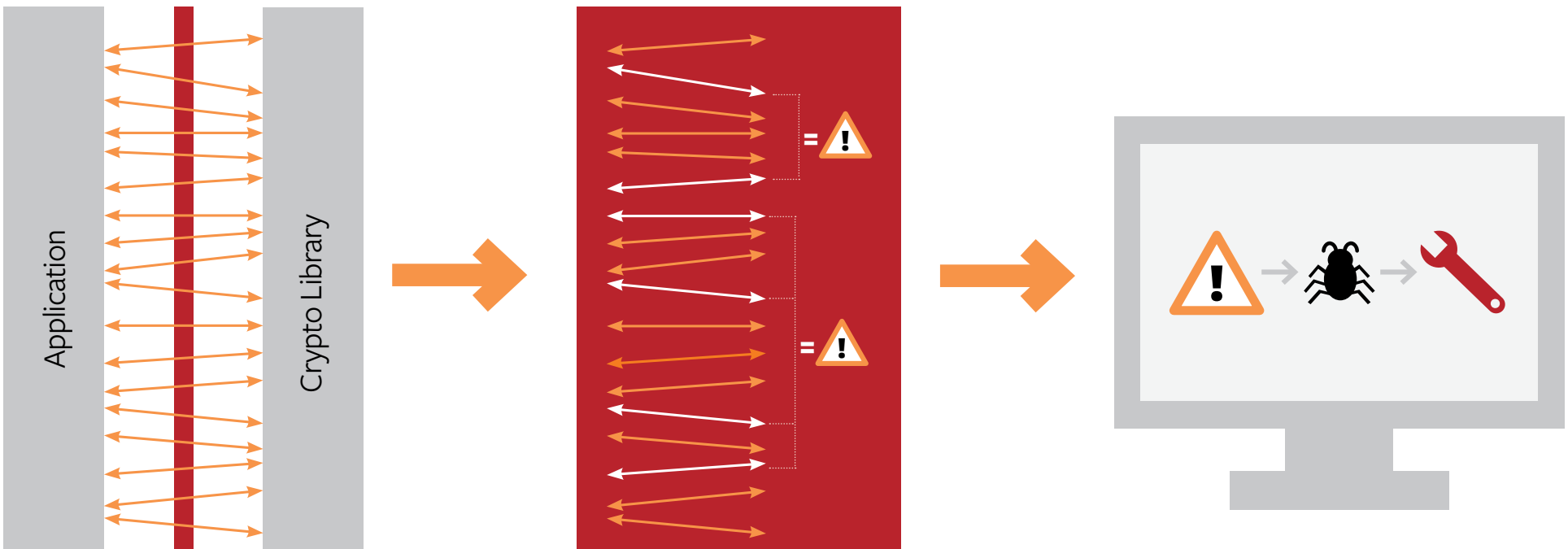


1. Tracing

2. Analysis*

* Either on-premise or in the cloud as SAAS

Reports are shown in a web interface with **links to stacktraces** for fast debugging and compliance analysis to ENISA, NIST, PCI-DSS or a custom crypto policy.



1. Tracing

2. Analysis*

3. Remediation*

* Either on-premise or in the cloud as SAAS

Try it for yourself

testmycrypto.com

Cryptosense

Academic spin-off (2013)

Current clients

Funding bodies

Prizes

Graham Steel, PhD
CEO & Founder

Inria informatics mathematics

Università Ca'Foscari Venezia

- 3 of top 5 European Banks
- 2 SIFIs (Financial Services Infrastructure Providers)
- US and French government agencies

IT-Translation

Elaia Partners

UBS Future of Finance 2015 Global Finalist

prix de l'innovation des assises 2016 Winner

Your Partner for Secure Crypto

https://cryptosense.com

graham@cryptosense.com

+33 (0)9 72 42 35 31

@cryptosense

Cryptosense