

RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: CRYPT-W03

Post-Snowden Cryptography

CHANGE

Challenge today's security thinking



MODERATOR:

Bart Preneel

Professor
KU Leuven/iMinds
bart.preneel@esat.kuleuven.be

PANELISTS:

Paul Kocher

President and Chief Scientist
Cryptography Research, Inc.

Adi Shamir

Professor
Weizmann Institute of Science

Hugo Krawczyk

Researcher
IBM T.J. Watson Research Center

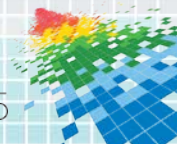
Nigel Smart

Professor
Dyadic Security/University of Bristol

Snowden Revelations



- ◆ NSA/GCHQ: “Collect it all, know it all, exploit it all”
 - ◆ most capabilities could have been extrapolated from open sources
- ◆ But still...
- ◆ massive scale and impact
 - ◆ redundancy: at least 3 methods to get to Google’s data
 - ◆ many other countries collaborated (beyond five eyes): economy of scale
 - ◆ industry collaboration through bribery, security letters, ...

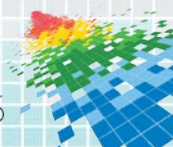




Surveillance is not passive but active

- ◆ **Active defense**
 - ◆ networks
 - ◆ Quantum insertion: answer before the legitimate website
 - ◆ FoxAcid: specific malware
 - ◆ devices
 - ◆ supply chain subversion
- ◆ Translation in human terms: **complete control** of networks and systems, including bridging the air gaps

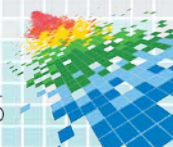
- ◆ No longer deniable





Undermining Cryptography

- Undermining standards
 - Going after keys (public and private)
 - Weak implementations
 - Cryptanalysis
-
- Increasing complexity of standards
 - Export controls
 - Hardware backdoors
 - Work with law enforcement to promote backdoor access and data retention



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: CRYPT-W03

Post-Snowden Cryptography

CHANGE

Challenge today's security thinking



MODERATOR:

Bart Preneel

Professor
KU Leuven/iMinds
bart.preneel@esat.kuleuven.be

PANELISTS:

Paul Kocher

President and Chief Scientist
Cryptography Research, Inc.

Adi Shamir

Professor
Weizmann Institute of Science

Hugo Krawczyk

Researcher
IBM T.J. Watson Research Center

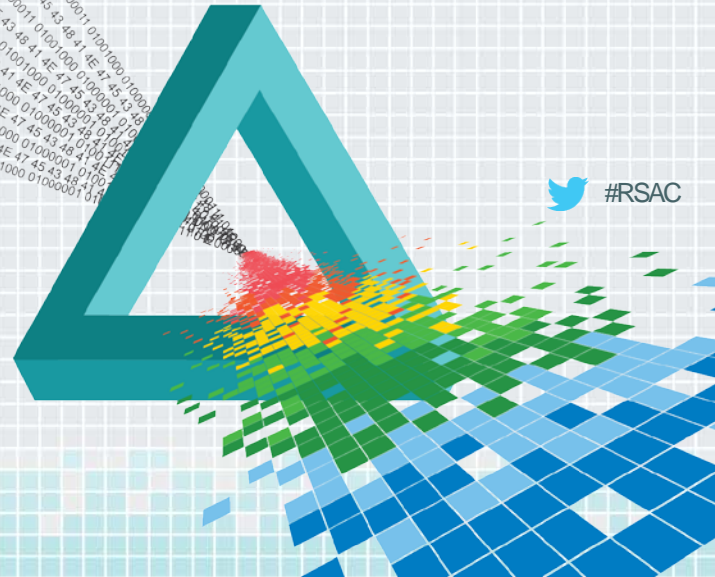
Nigel Smart

Professor
Dyadic Security/University of Bristol

RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Thank You



 #RSAC