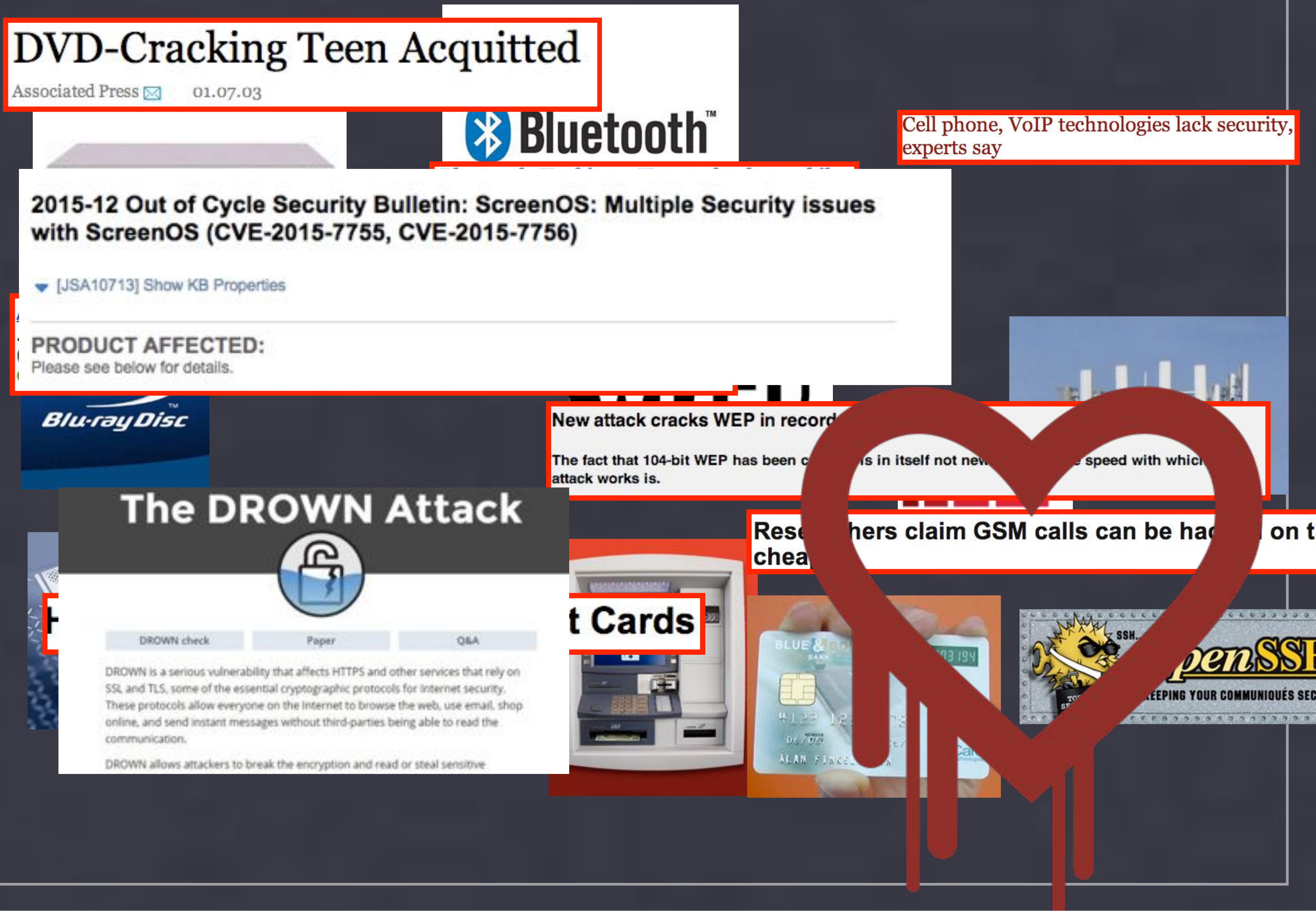
601.445/645 Practical Cryptographic Systems

Introduction

Instructor: Matthew Green

Intro

- What is a Cryptographic System?
  - A security system
  - Uses cryptography
- Many fascinating ways to get it wrong!
  - “Practical”:
    People actually use it & depend on it



DVD-Cracking Teen Acquitted

Associated Press 01.07.03

Cell phone, VoIP technologies lack security, experts say

2015-12 Out of Cycle Security Bulletin: ScreenOS: Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756)

[JSA10713] Show KB Properties

PRODUCT AFFECTED:

Please see below for details.

New attack cracks WEP in record

The fact that 104-bit WEP has been c is in itself not new speed with which attack works is.

The DROWN Attack

DROWN check | Paper | Q&A

DROWN is a serious vulnerability that affects HTTPS and other services that rely on SSL and TLS, some of the essential cryptographic protocols for Internet security. These protocols allow everyone on the Internet to browse the web, use email, shop online, and send instant messages without third-parties being able to read the communication.

DROWN allows attackers to break the encryption and read or steal sensitive

Rese hers claim GSM calls can be ha on t chea

t Cards

Motivation

- Building (successful) systems requires more than cryptographic expertise
  - Though it’s a prerequisite!
- It’s cross-disciplinary:
  - Crypto
  - Information Security
  - Software Engineering
  - Hardware Engineering
  - UI, Policy, etc...

This course

- Not a course in theoretical cryptography
  - We’ll cover cryptography from a practical angle, aim is to apply cryptography
- Practice-oriented tutorial
  - examine how systems fail
  - how we can design against it
  - what can’t we design against
- Driven by your questions & the news

What you’ll come away with

- A grounding in cryptographic techniques
  - The right algorithms
  - Strengths & weaknesses, applicability
  - A feel for the design/evaluation process
  - Introduction to standards (e.g., FIPS)
  - Enough to know where to look for more
- Knowledge of our own limitations
  - Building secure systems is hard
    (even for experts)

Grading, Text

- Grading Policy:
  - 40% Exams (Midterm & Final)
  - 40% Assignments
  - 15% Project
  - 5% Class participation
- Texts:
  - Katz/Lindell: Modern Cryptography
  - Anderson: Security Engineering
- Website: spar.isi.jhu.edu/~mgreen/650.445

Electronic Stuff & Reading

- Website
  - http://spar.isi.jhu.edu/~mgreen/650.445/
    (or just Google "Practical Cryptographic Systems")
  - Slides up as we go
  - Reading assignment today (for Weds)
    Anderson chap 5.7 (Symmetric Crypto)
  - My Office Hours Weds 2:30-3:30pm
  - TA Office Hours (TBD but soon)
  - Assignment 1 out today (2:00pm)

Programming

- The assignments in this class involve writing code
  - We will primarily use Go
(with exceptions)
  - It’s your responsibility to give us working assignments that build/run
  - Anything other than a working assignment is a failure

Course Guidelines

- Do:
  - Read the news!
    Twitter, Slashdot, ArsTechnica, etc.
  - Bring up interesting topics & recent attacks you'd like to learn more about
- Don't:
  - Cheat***
  - Get me arrested

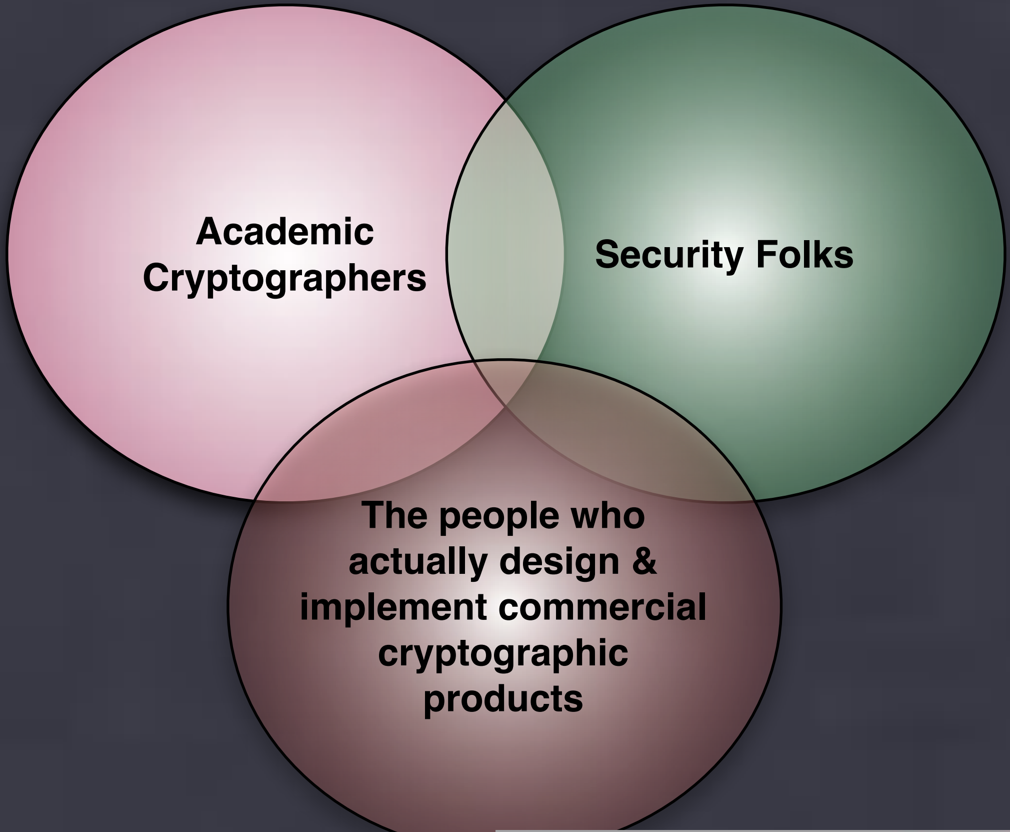
Readings

- Assigned each week
  - You must read them, be prepared to discuss in class
  - These wil be covered in written assignments on the homework, as well as exams

Incidentals

- Piazza page
  - Join it! (piazza.com - JHU - course name)
- Travel
  - From time to time I might not be here
  - Someone else will cover for me
  - I’m going to assign reading!

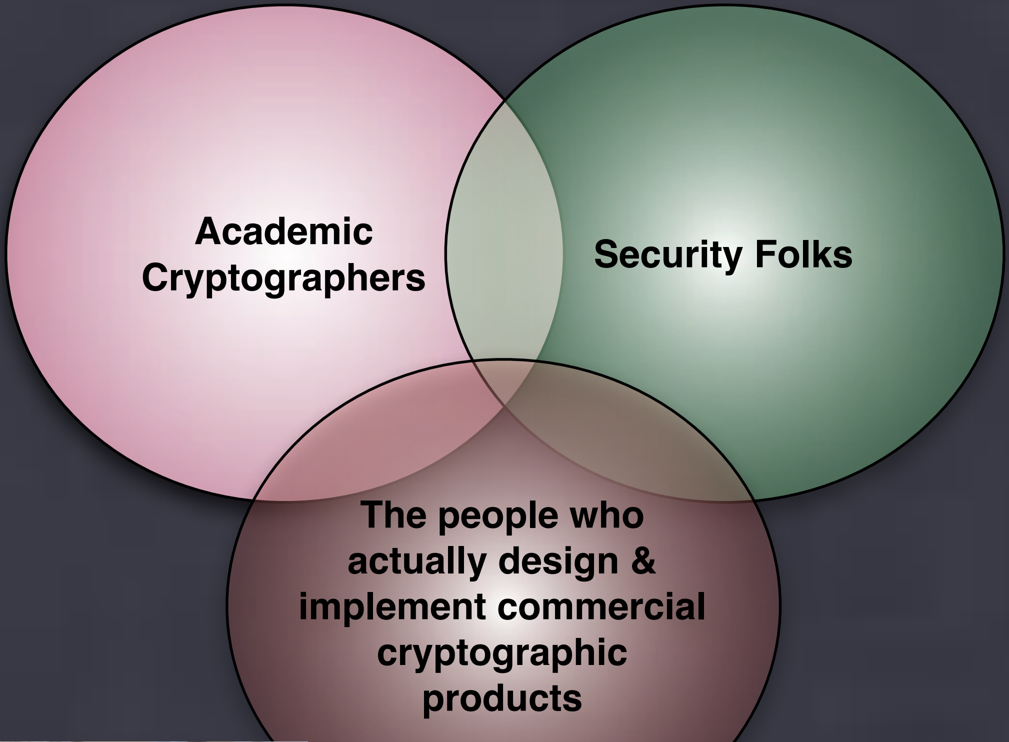
Today



Academic Cryptographers

Security Folks

The people who actually design & implement commercial cryptographic products



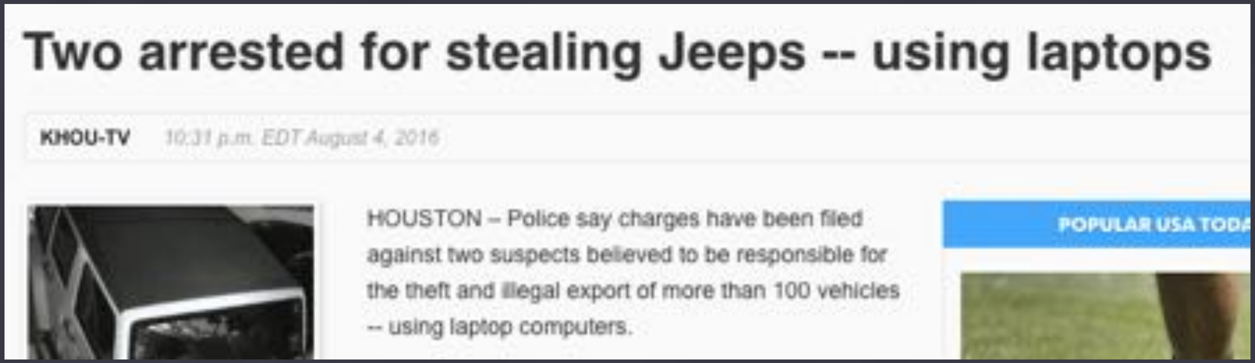
Academic Cryptographers

Security Folks

The people who actually design & implement commercial cryptographic products

Security Failure

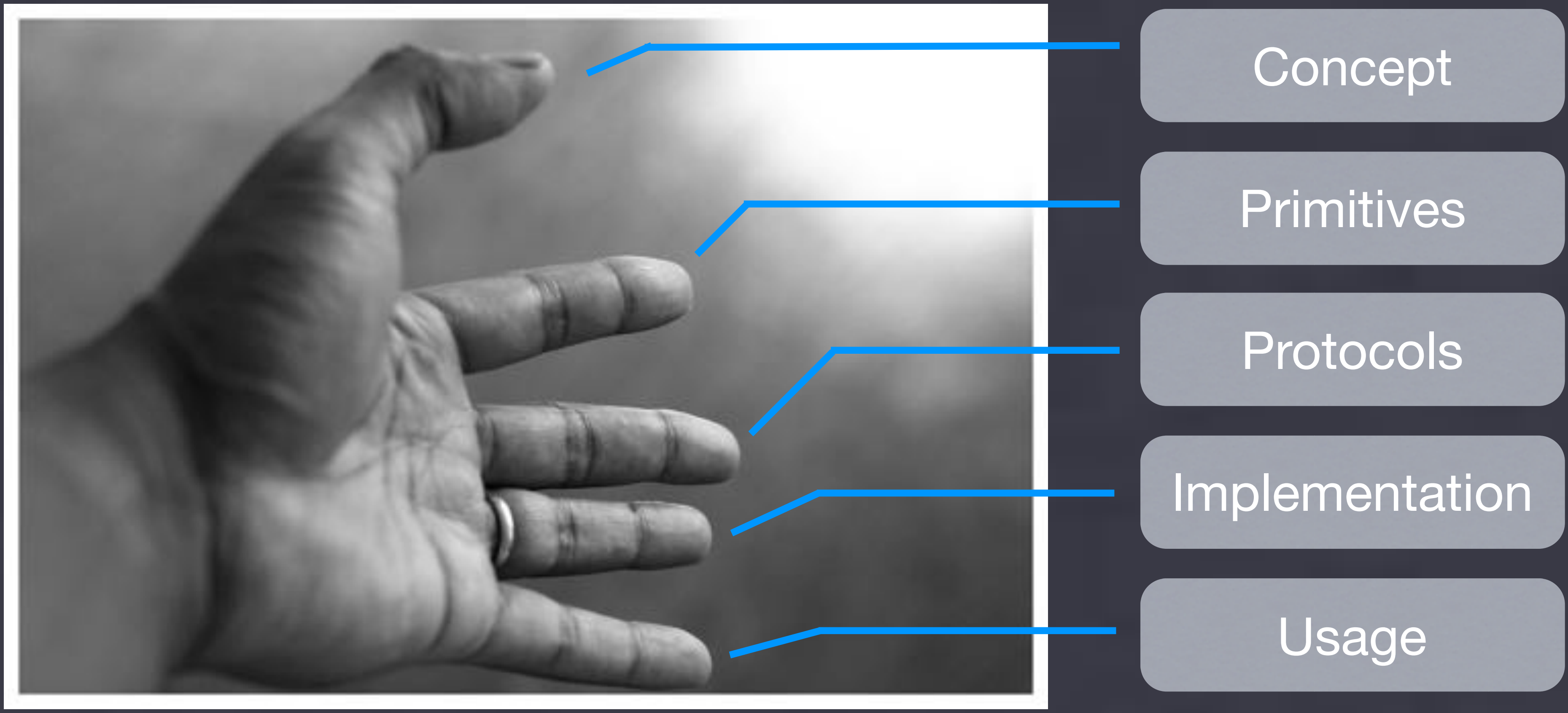
- When systems fail:
  - Researchers get published
  - $$$ lost
  - Private information compromised
  - People die (?)



Two arrested for stealing Jeeps -- using laptops

KHOU-TV 10:31 p.m. EDT August 4, 2016

HOUSTON – Police say charges have been filed against two suspects believed to be responsible for the theft and illegal export of more than 100 vehicles -- using laptop computers.



Concept

Primitives

Protocols

Implementation

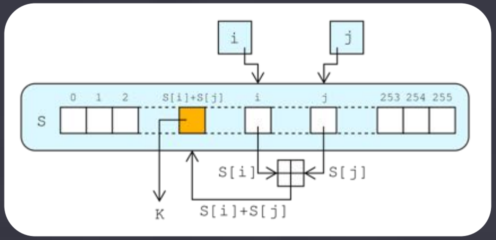
Usage

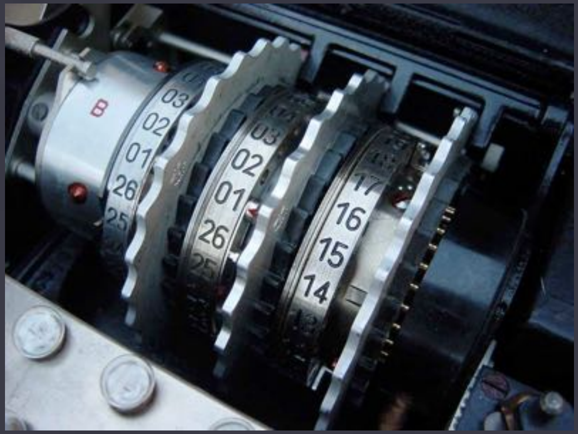
Photo by Flickr user Studio Antwan used under a Creative Commons license

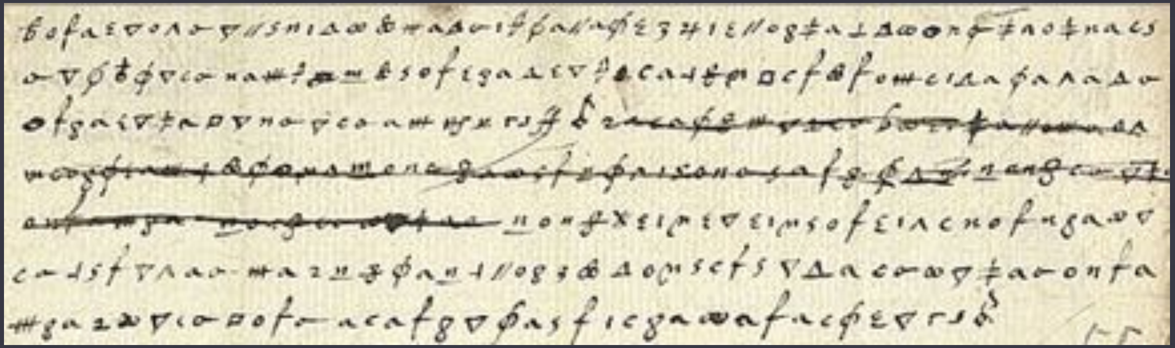
Primitives

Primitives

- **Codes, ciphers, encryption schemes, MACs, etc.:**
  - **Classically, an attack on the “system” meant an attack on the primitive**
  - **History is littered with broken primitives**

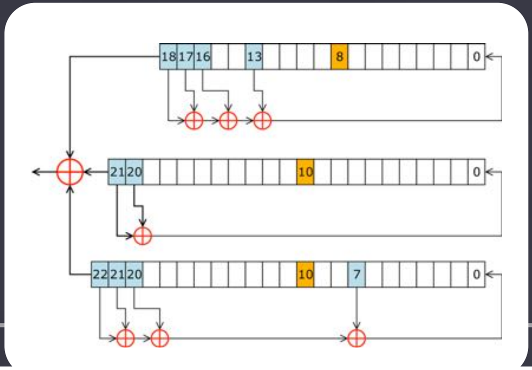






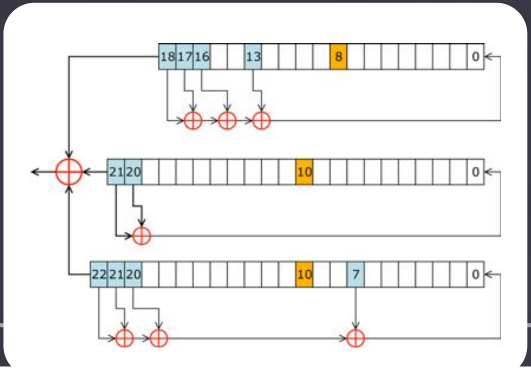
Primitives

- **Practical Example: GSM encryption**
  - **A5/0: No encryption**
  - **A5/1: Based on LFSRs**
  - **A5/2: Weakened A5/1**
  - **A5/3 (KASUMI): New for 3G**



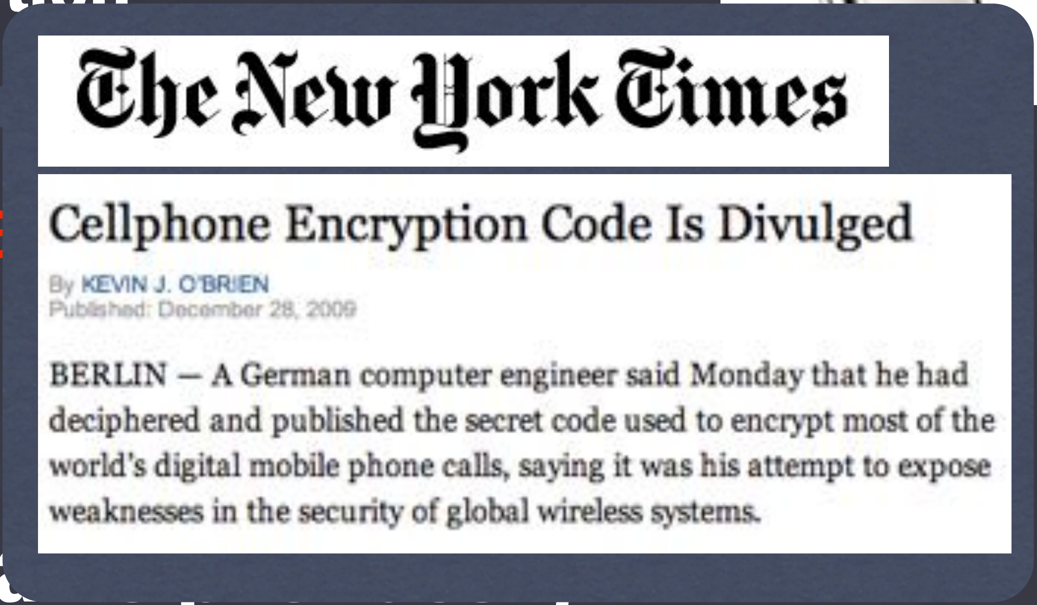
Primitives

- Practical Example: GSM encryption
  - A5/0: No encryption
  - A5/1: Broken
  - A5/2: Way Broken
  - A5/3 (KASUMI): Dented (and 3G vuln. to protocol attacks)
- Deliberately weak cipher design
  - Cost & politics



Primitives

- Practical Example: GSM encryption
  - A5/0: No encryption
  - A5/1: Broken
  - A5/2: Way Broke
  - A5/3 (KASUMI): (and 3G vuln. to
- Deliberately wea
  - Cost & politics



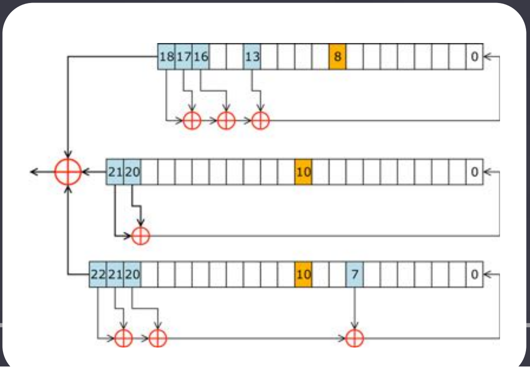
The New York Times

Cellphone Encryption Code Is Divulged

By KEVIN J. O'BRIEN
Published: December 28, 2009

BERLIN — A German computer engineer said Monday that he had deciphered and published the secret code used to encrypt most of the world's digital mobile phone calls, saying it was his attempt to expose weaknesses in the security of global wireless systems.

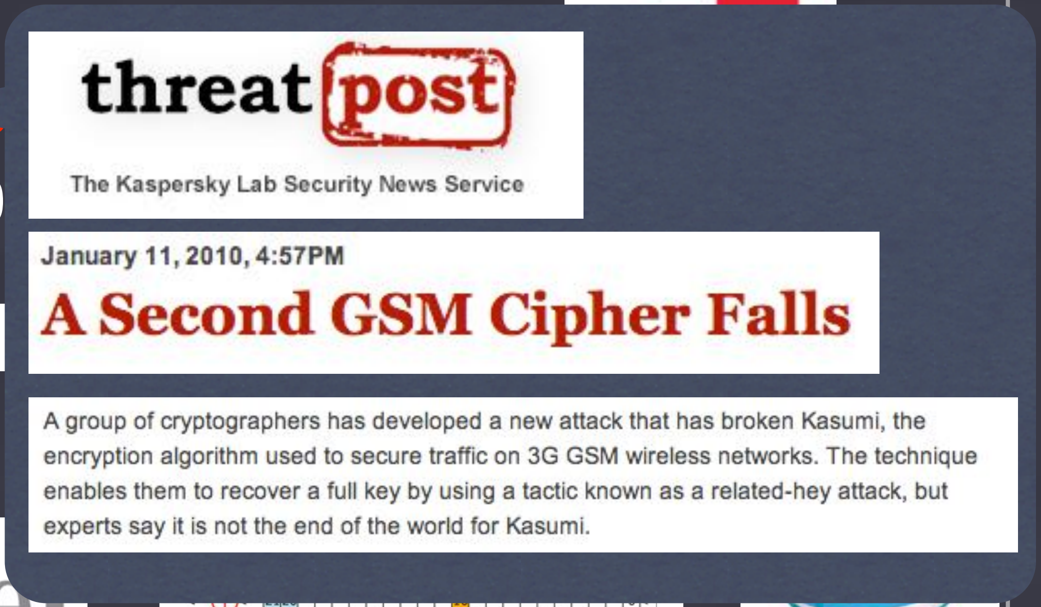
T · · Mobile



at&t

Primitives

- Practical Example: GSM encryption
  - A5/0: No encryption
  - A5/1: Broken
  - A5/2: Way Broken
  - A5/3 (KASUMI): Dente
    (and 3G vuln. to proto
- Deliberately weak ci
  - Cost & politics



threat post

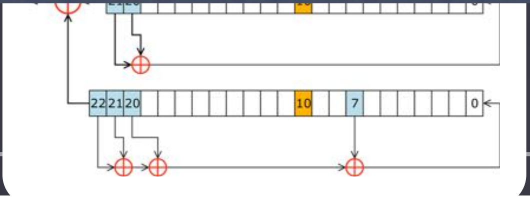
The Kaspersky Lab Security News Service

January 11, 2010, 4:57PM

A Second GSM Cipher Falls

A group of cryptographers has developed a new attack that has broken Kasumi, the encryption algorithm used to secure traffic on 3G GSM wireless networks. The technique enables them to recover a full key by using a tactic known as a related-hey attack, but experts say it is not the end of the world for Kasumi.

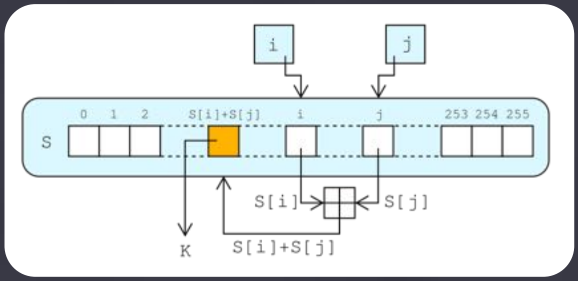
T · · Mobile

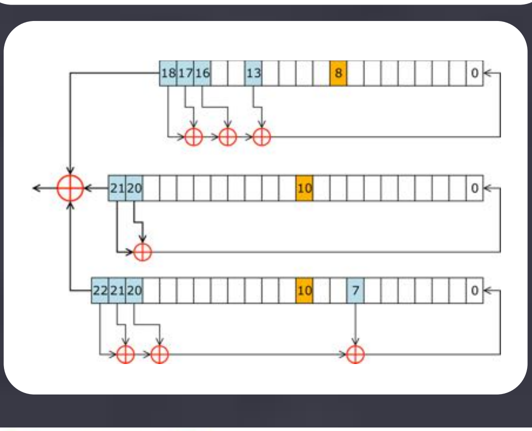


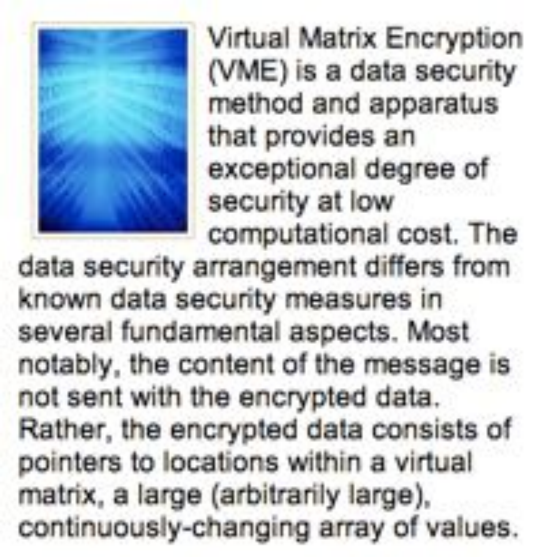
at&t

Primitives

- Typical problems:
  - Using the wrong ones (& homebrew crypto)
  - Or using the right ones... wrong
  - E.g., RC4 in WEP and TLS

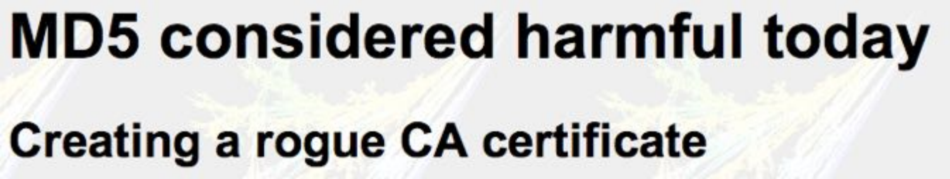





Virtual Matrix Encryption (VME) is a data security method and apparatus that provides an exceptional degree of security at low computational cost. The data security arrangement differs from known data security measures in several fundamental aspects. Most notably, the content of the message is not sent with the encrypted data. Rather, the encrypted data consists of pointers to locations within a virtual matrix, a large (arbitrarily large), continuously-changing array of values.

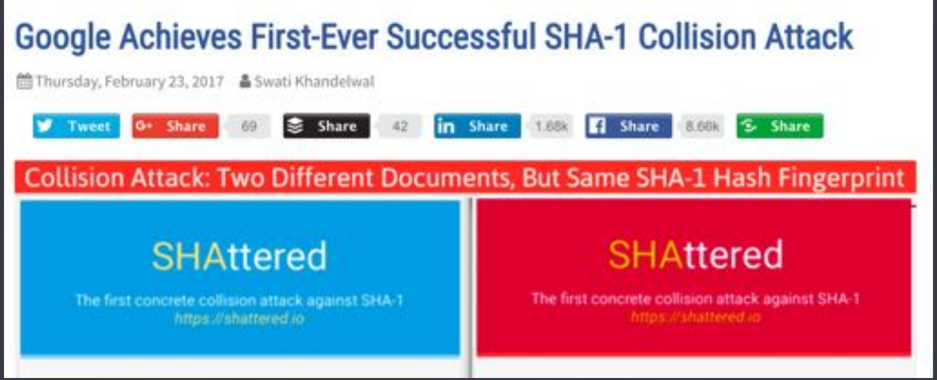
Primitives

- Sometimes the “right” primitives stop being right…
    - The great Hash Function Adventure of 2000-2017
(MD5 broken, SHA1 broken)



MD5 considered harmful today

Creating a rogue CA certificate



Google Achieves First-Ever Successful SHA-1 Collision Attack

Thursday, February 23, 2017 Swati Khandelwal

Collision Attack: Two Different Documents, But Same SHA-1 Hash Fingerprint

SHAttered

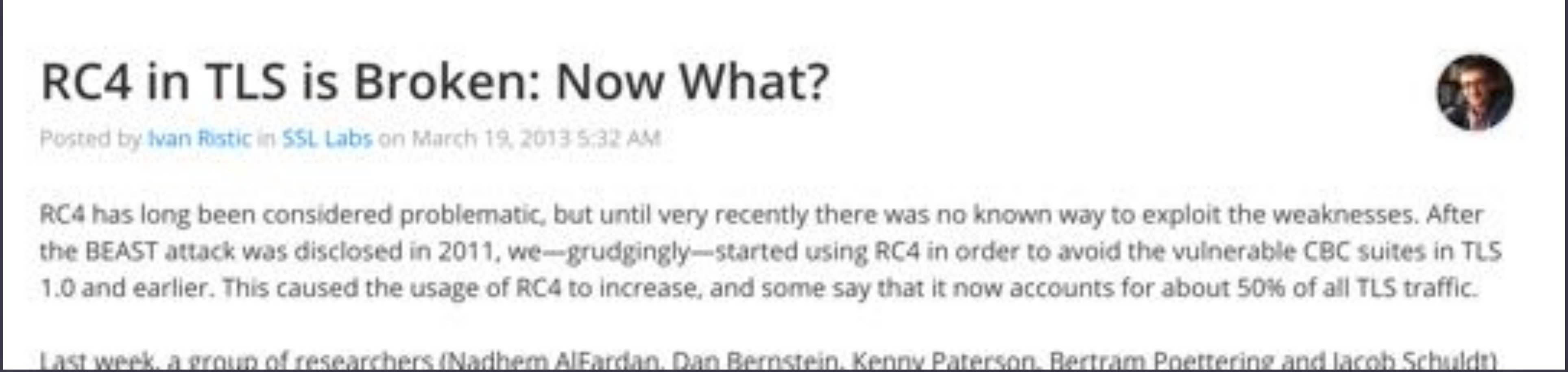
The first concrete collision attack against SHA-1
https://shattered.io

SHAttered

The first concrete collision attack against SHA-1
https://shattered.io

Primitives

- **Sometimes the “right” primitives stop being right…**
  - **More recently:**



RC4 in TLS is Broken: Now What?

Posted by Ivan Ristic in SSL Labs on March 19, 2013 5:32 AM

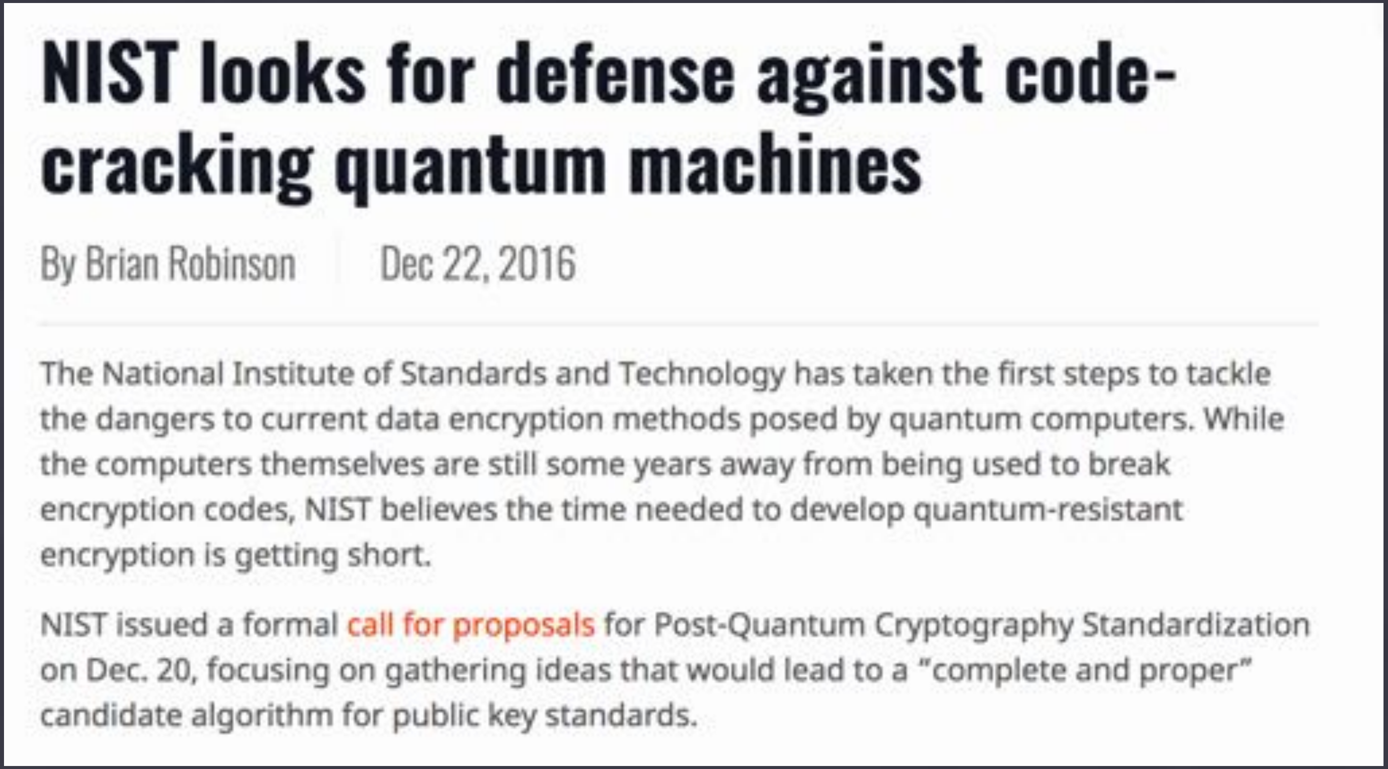
RC4 has long been considered problematic, but until very recently there was no known way to exploit the weaknesses. After the BEAST attack was disclosed in 2011, we—grudgingly—started using RC4 in order to avoid the vulnerable CBC suites in TLS 1.0 and earlier. This caused the usage of RC4 to increase, and some say that it now accounts for about 50% of all TLS traffic.

Last week, a group of researchers (Nadhem AlFardan, Dan Bernstein, Kenny Paterson, Bertram Poettering and Jacob Schuldt)

AES Image Source: http://www.quadibloc.com/crypto/co0404.htm

Primitives

- Sometimes the "right" primitives stop being right...



NIST looks for defense against code-cracking quantum machines

By Brian Robinson | Dec 22, 2016

The National Institute of Standards and Technology has taken the first steps to tackle the dangers to current data encryption methods posed by quantum computers. While the computers themselves are still some years away from being used to break encryption codes, NIST believes the time needed to develop quantum-resistant encryption is getting short.

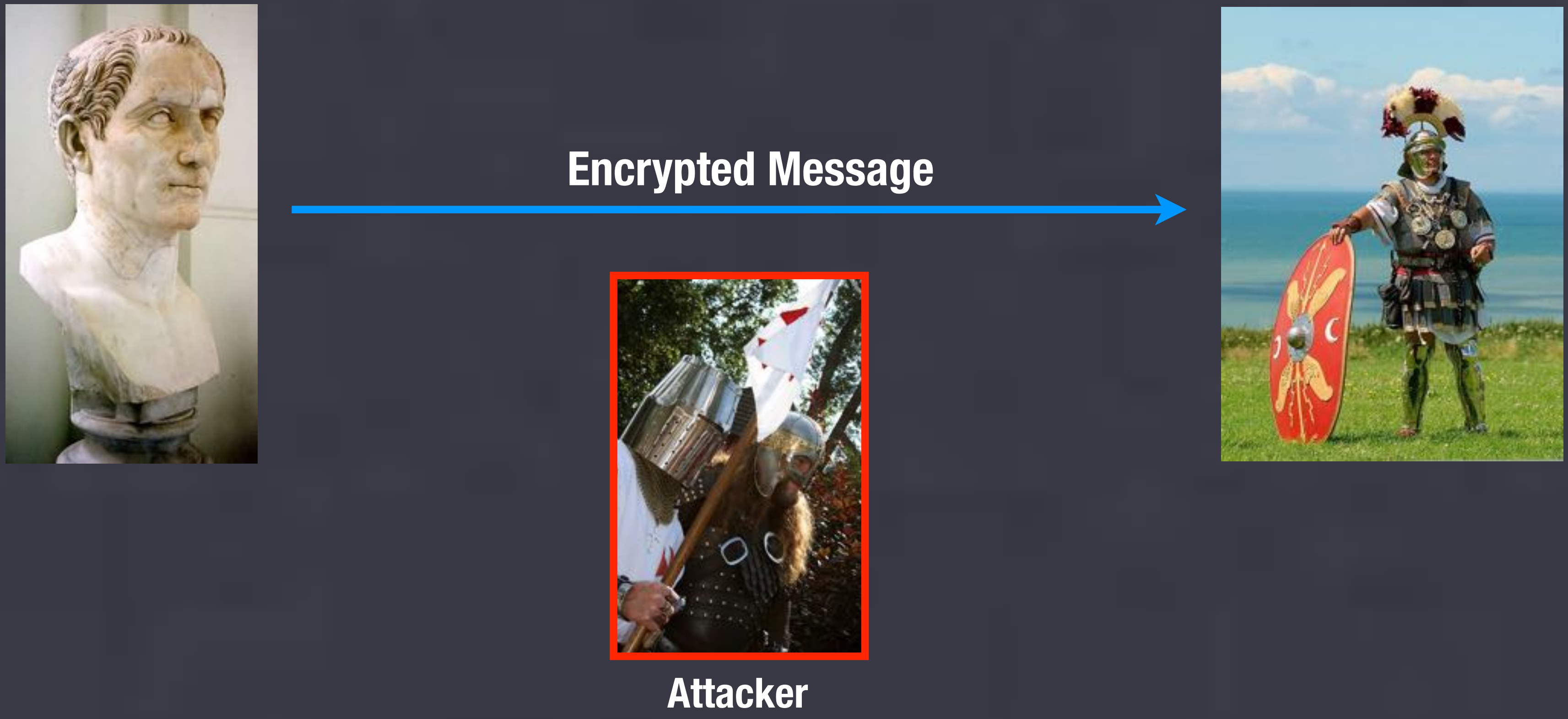
NIST issued a formal call for proposals for Post-Quantum Cryptography Standardization on Dec. 20, focusing on gathering ideas that would lead to a "complete and proper" candidate algorithm for public key standards.

AES Image Source: http://www.quadibloc.com/crypto/co0404.htm

Protocols

Protocols

- **Classical cryptographic protocol:**



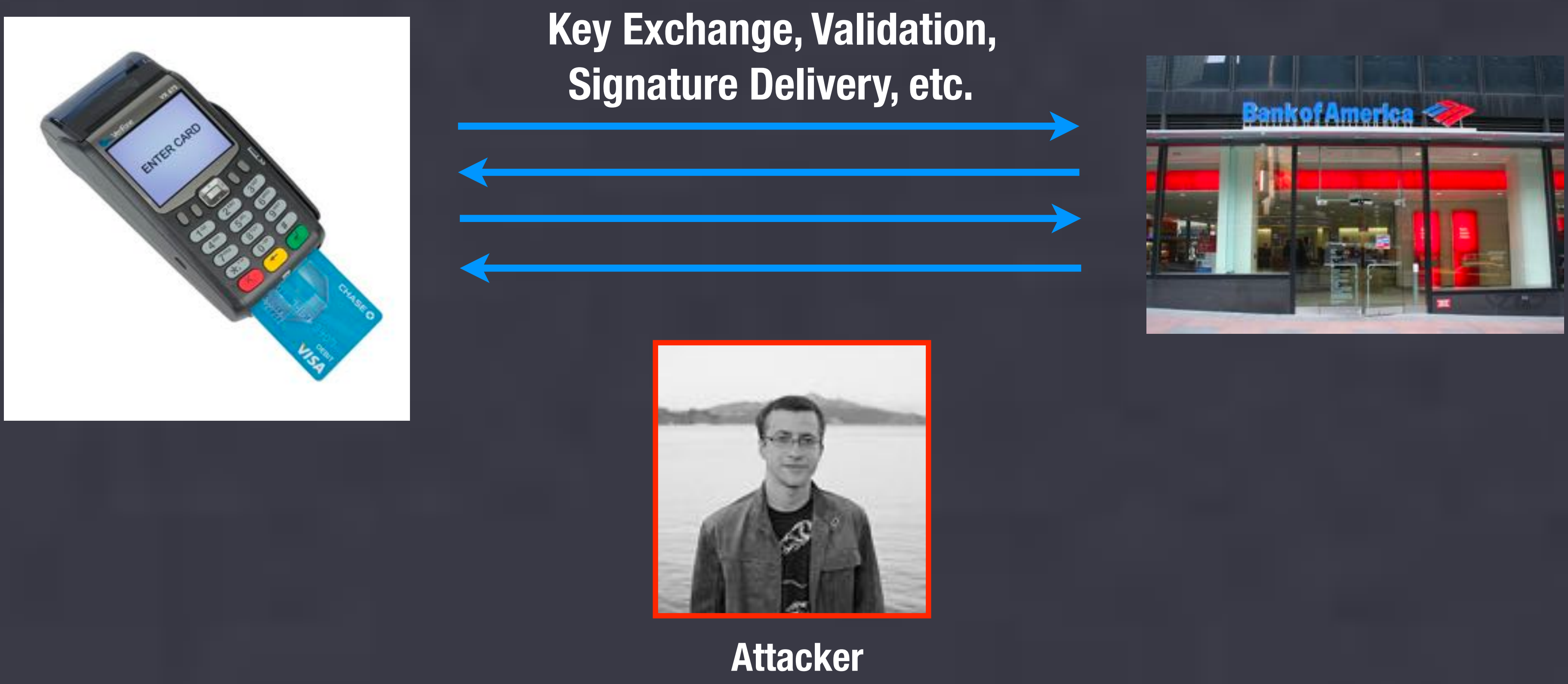
Encrypted Message

Attacker

Caesar, Centurion: Wikipedia. Barbarians by Flickr user skitzianist used under a Creative Commons license.

Protocols

- **Modern cryptographic protocol:**



Key Exchange, Validation, Signature Delivery, etc.

Attacker

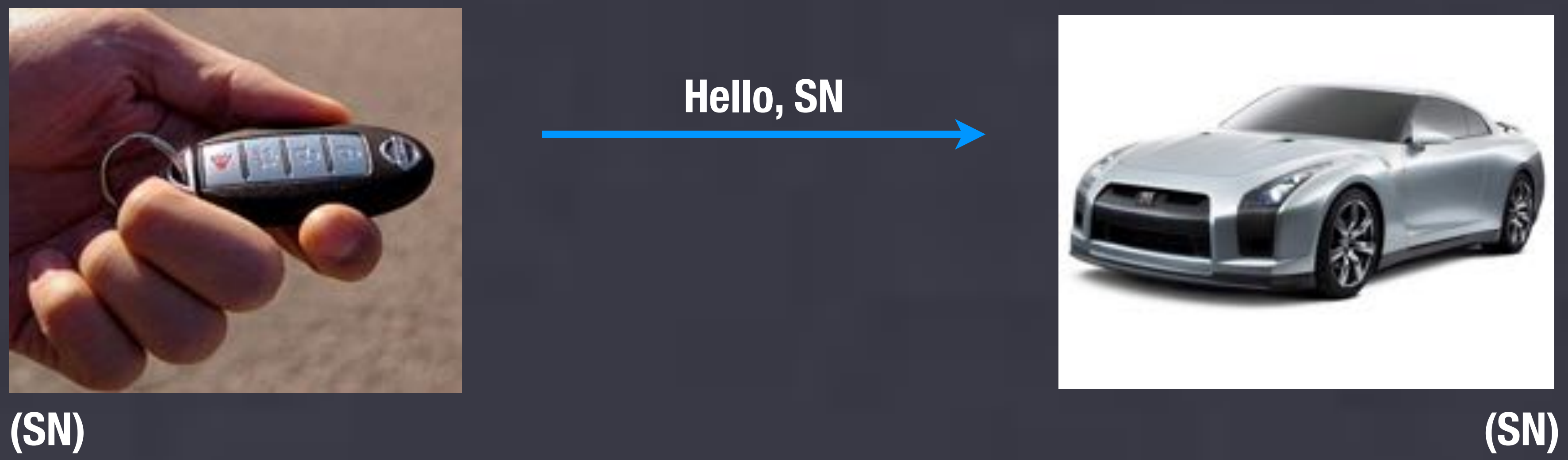
Image of Jon Johansen from http://nanocr.eu/picture.php, used under a Creative Commons license.

Protocol examples:

- **Vehicle remote control/immobilizer**
  - **Only legitimate owner can start the car/ unlock the doors, etc.**

Protocol examples:

- Vehicle remote control/immobilizer
  - Early systems used fixed Serial Number



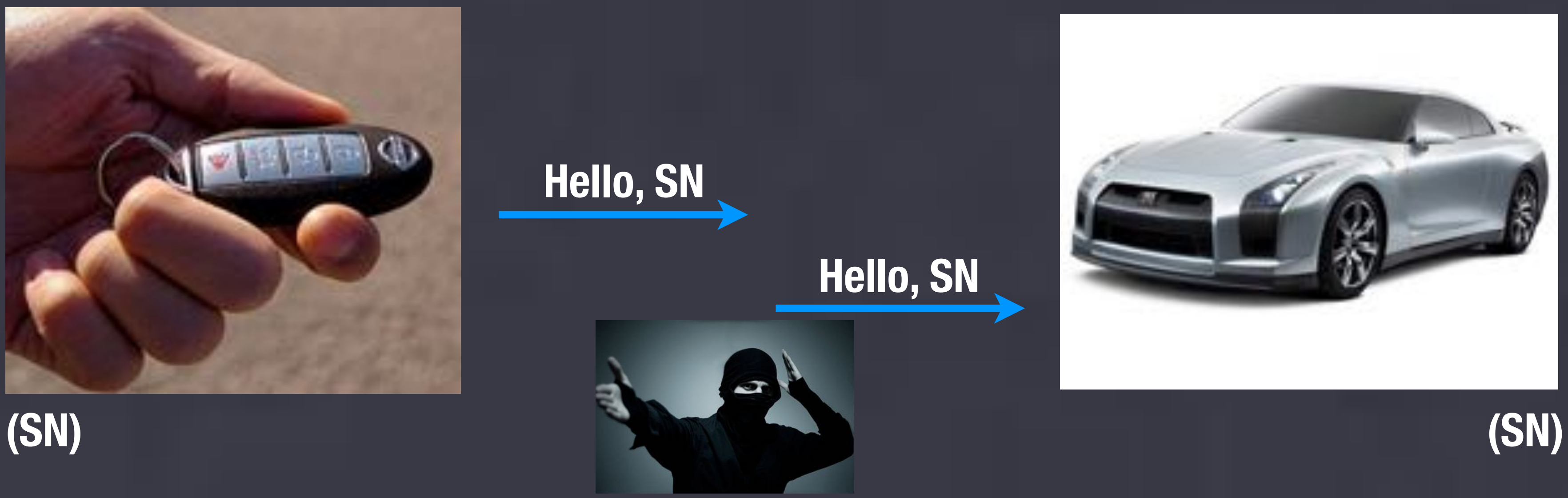
Hello, SN

(SN)

(SN)

Protocol examples:

- Vehicle remote control/immobilizer
  - Early systems used fixed Serial Number
  - Vulnerable to “replay attack”



Hello, SN

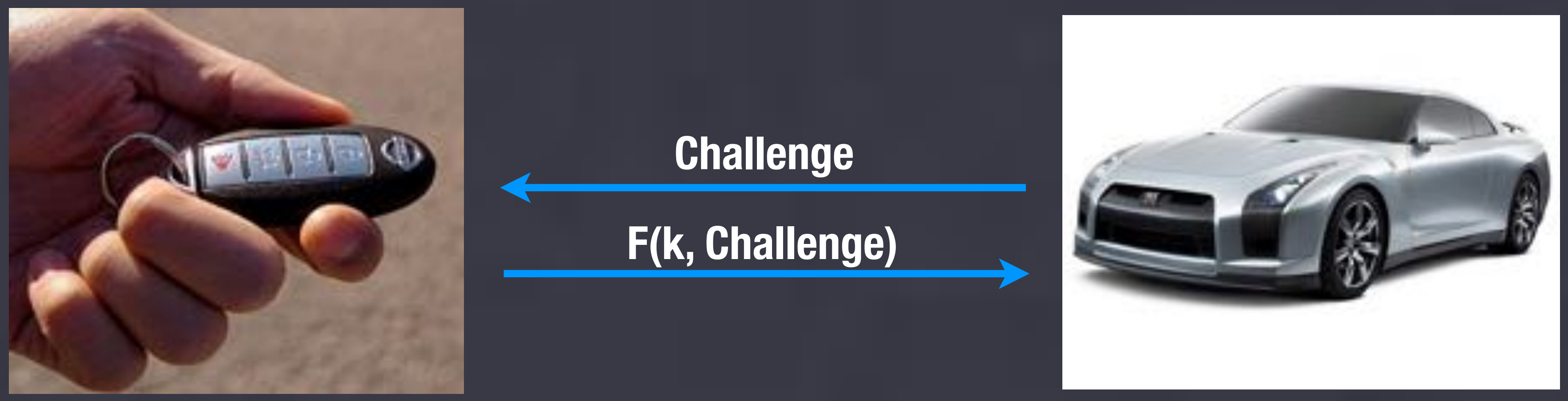
Hello, SN

(SN)

(SN)

Protocol examples:

- **Solution: Challenge-Response**
  - “Identification Friend or Foe”
  - Key is never broadcast over the air



Challenge

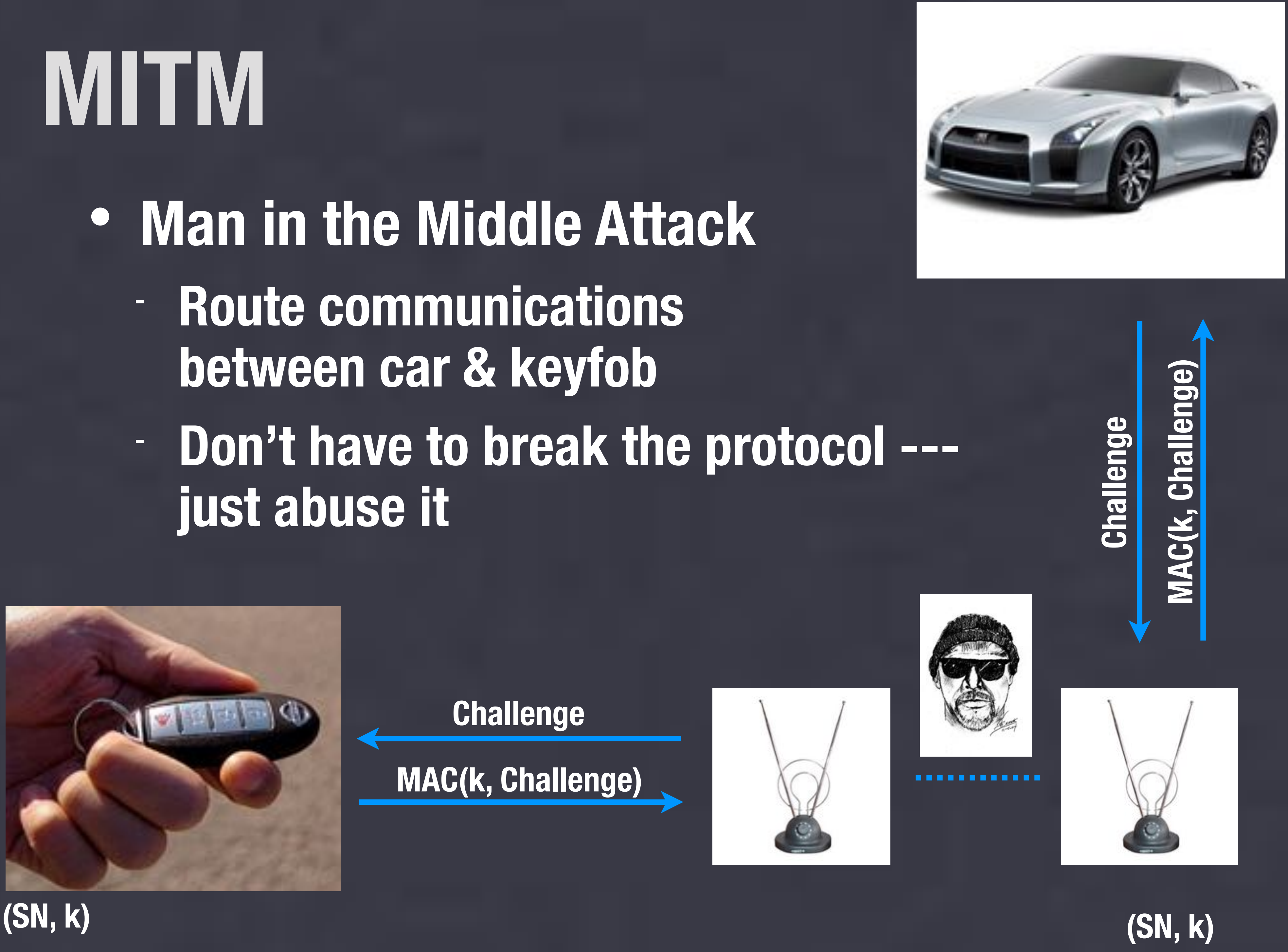
F(k, Challenge)

(SN, k)

(SN, k)

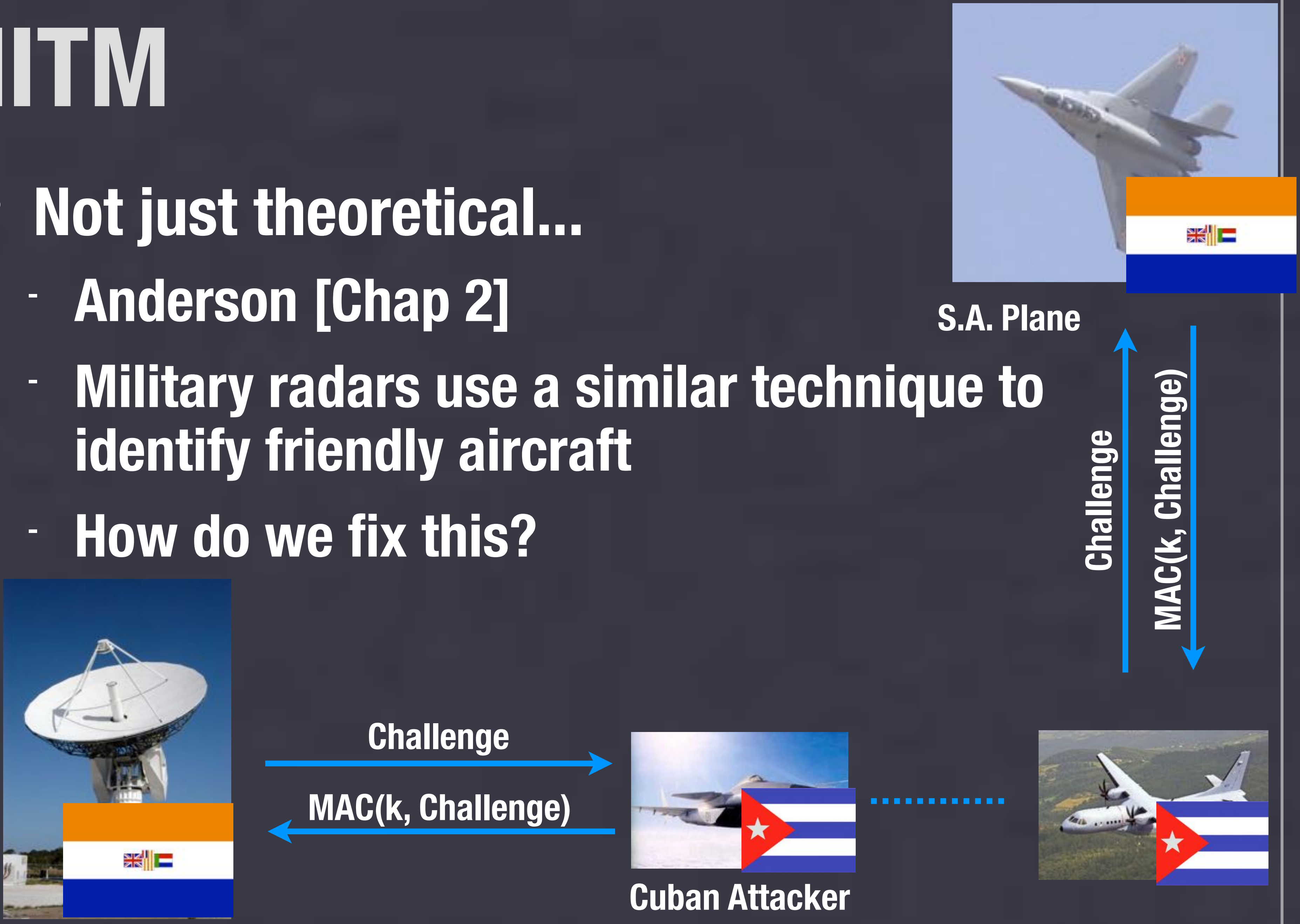
MITM

- Man in the Middle Attack
  - Route communications between car & keyfob
  - Don’t have to break the protocol --- just abuse it



MITM

- Not just theoretical...
  - Anderson [Chap 2]
  - Military radars use a similar technique to identify friendly aircraft
  - How do we fix this?



S.A. Plane

Challenge

MAC(k, Challenge)

Challenge

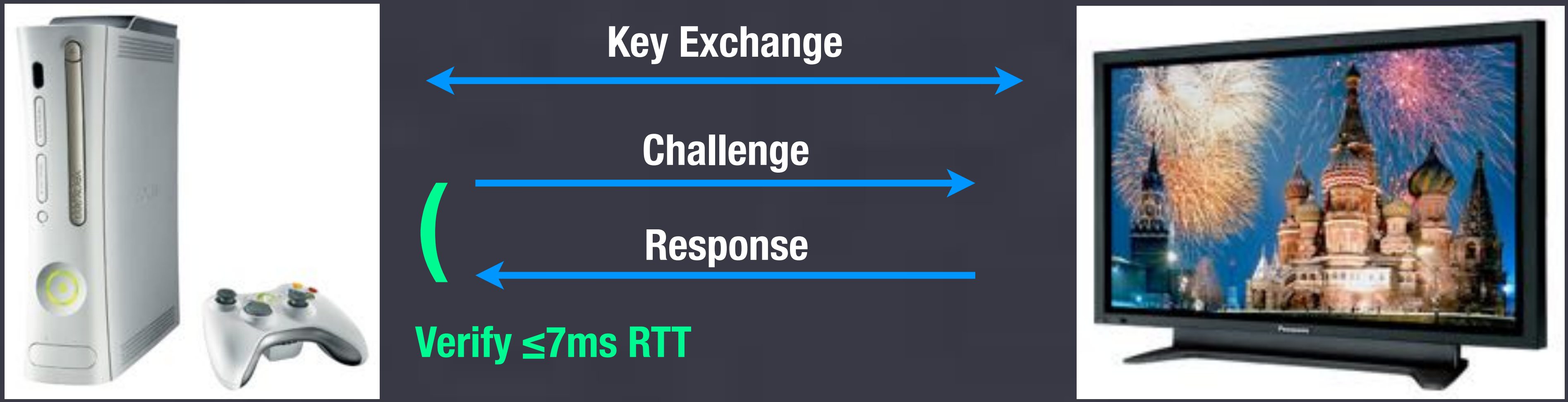
MAC(k, Challenge)

Cuban Attacker

S.A. Radar

Round Trip Timing

- The case of DTCP-IP
  - Content transport protocol
  - Concern: prevent user from sharing content over the Internet
  - Ensure that Sink is within 7ms of Source



Key Exchange

Challenge

Response

Verify ≤7ms RTT

Source

Sink