

# **Master in BIG DATA IN BUSINESS**

**cybersecurity-related content:**

**security and privacy  
blockchain technologies & applications**

*Giuseppe Bianchi*

*giuseppe.bianchi@uniroma2.it*

*Università di Roma Tor Vergata*

# S&P in big data: what's the problem?

**Military-grade encryption + access control, that's it!**

The incompetence of unskilled people  
metacognitive ability to  
are incompetent

## Dunning-Kruger Effect



being ignorant  
nature of ignorance

World examples!  
School, work, working groups,...

Who are unskilled in these  
tasks and make  
conclusions and make  
ability to realize it. Across 4  
tests of humor, grammar, and  
test scores put them in the  
lowest. I linked this miscalibration  
from error. Paradoxically,  
competence, helped them

# Security and Privacy: huge topic!

## → Several 'dimensions'

- ⇒ Network security, perimetral protection, monitoring, ...
- ⇒ Systems security, vulnerability assessment, forensics
- ⇒ Storage / data base security, data protection, access control
- ⇒ Auditing, security assurance, risk assessment, certification
- ⇒ Security data analytics, data mining, intelligence analytics
- ⇒ Visibility of security & visualization
- ⇒ Secure computation privacy preserving data mining
- ⇒ Etc etc etc... (!!)

## → Before all this... need for (at least!) very basic crypto and system security background

## → So... how to fit into as little as 18 + 9 h????!!

- ⇒ And have something practical  
(e.g. beyond just a basic crypto or vulnerability class...)

# Our approach / 1

→ **Do NOT teach crypto, BUT learn how (good) crypto can be poorly used**

⇒ Driving use case scenario: Web security (TLS)

→ **A lot (!) of broader take home messages!**

## **Examples:**

⇒ Security features negotiation?

→ Prevent bidding-down attacks!

⇒ Compress then encrypt?

→ CRIME attack, 2012!

⇒ MAC then encrypt?

→ Padding oracles (2002,2013,2015, 2016)

→ Very similar issues in other applications and scenarios

⇒ Implementation issues & side channels may play havoc!

→ ROBOT, 2018

→ Transient Execution attacks, 2018+

# Our approach / 2

## → Practical system security

⇒ Hands on laboratory (with kali linux):

→ learn how attackers think, what they use, how they act (very practical, a few penetration examples)

## → Take home:

**system security is not easy**

⇒ What about data-centric security?

Some very preliminary insights...

# Our approach / 3

## → Secure storage?

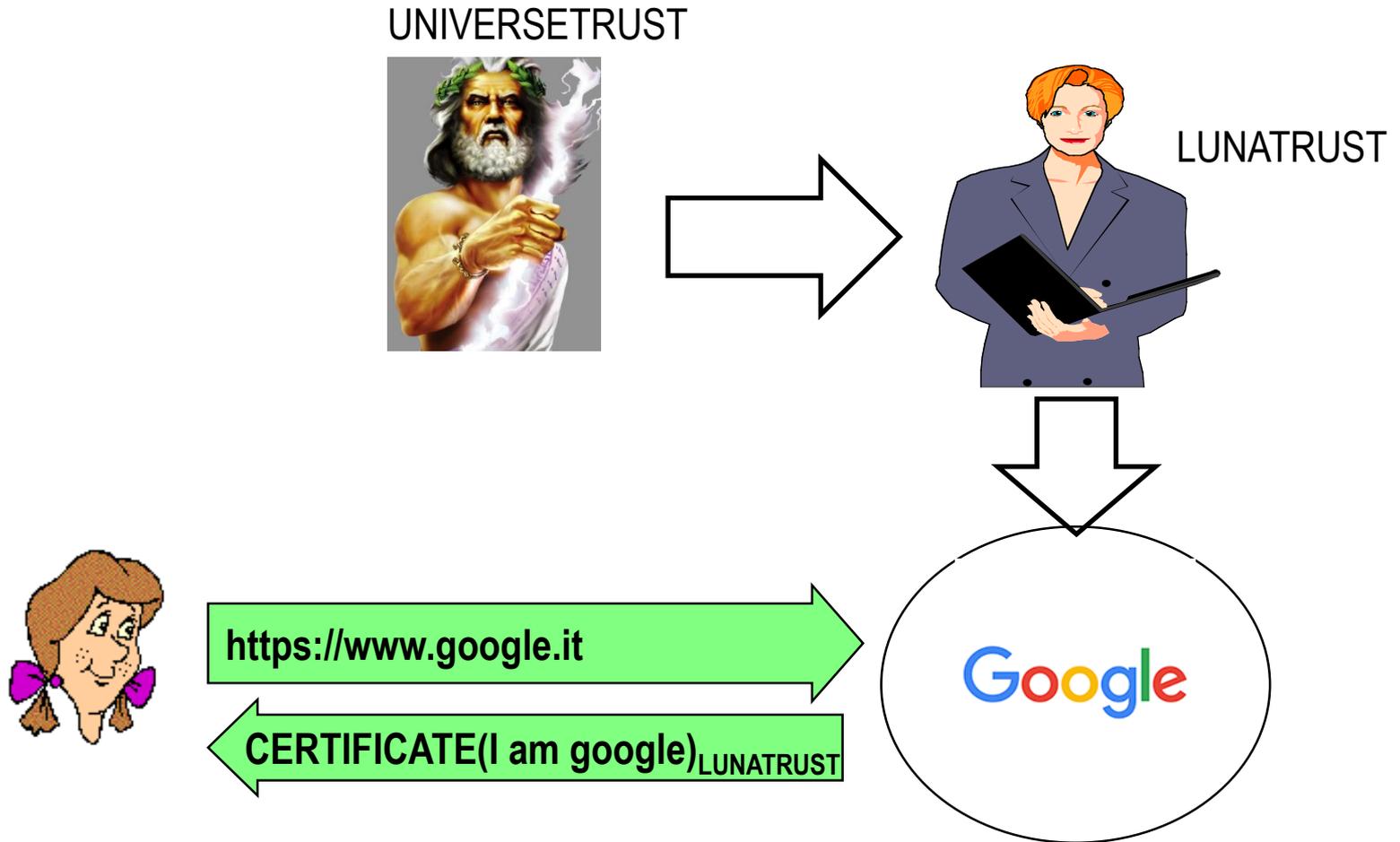
⇒ Hash-based data structures, Merkle trees

⇒ In Blockchain class, but not only blockchains

→ Big data example: Google's certificate transparency, for PKI security

→ **A real world example of a standard (though cleverly organized) DB which most would today call «blockchain», but which is NOT.**

# Web security pillar: Certificate Authorities ARE trusted!



# Fact: trusted CA assumption at stake

Fake SSL certificates  
threats, say



Online Security Blog

The latest news and insights from Google on security and safety on the Internet

Home News Anti-Phishing

## Fake SSL certificates

Netcraft has found dozens of fake SSL certificates. Some of these certificates may be used by attackers to impersonate legitimate websites and forward it to the bank. Successful attacks can result in the theft of authentication credentials, or more.

The fake certificates bear the same appearance as legitimate ones. As the certificates are not signed by a trusted CA, they are not recognized by browsers.

## Enhancing digital certificate security

Posted: Thursday, January 3, 2013



183



Tweet

300



Mi piace

by George Leopold

Published: 09 Jan 2015

Sections

Why 'b' SSL certificates

### → Google's VALID fake Certificates mistakenly (?) issued

→ by TurkTrust (2012), ANSSI France (2013), etc

### → Smaller CAs: compromised

⇒ Holland: Dgnotar

⇒ Malaysia: DigiCert sdn. Bhd.

⇒ etc

Engineer

ected and blocked an unauthorized digital certificate for the "\*.google.com" domain. We found the certificate was issued by an intermediate certificate authority (ICA) from a Turkish certificate authority. Intermediate CA certificates carry the full authority of the parent CA. This means that anyone who has one can use it to create a certificate for any website they wish to.

certificate revocation metadata on December 25 to block that intermediate CA, and to inform other browser vendors. TURKTRUST told us that based on our information, they had already revoked the certificate.

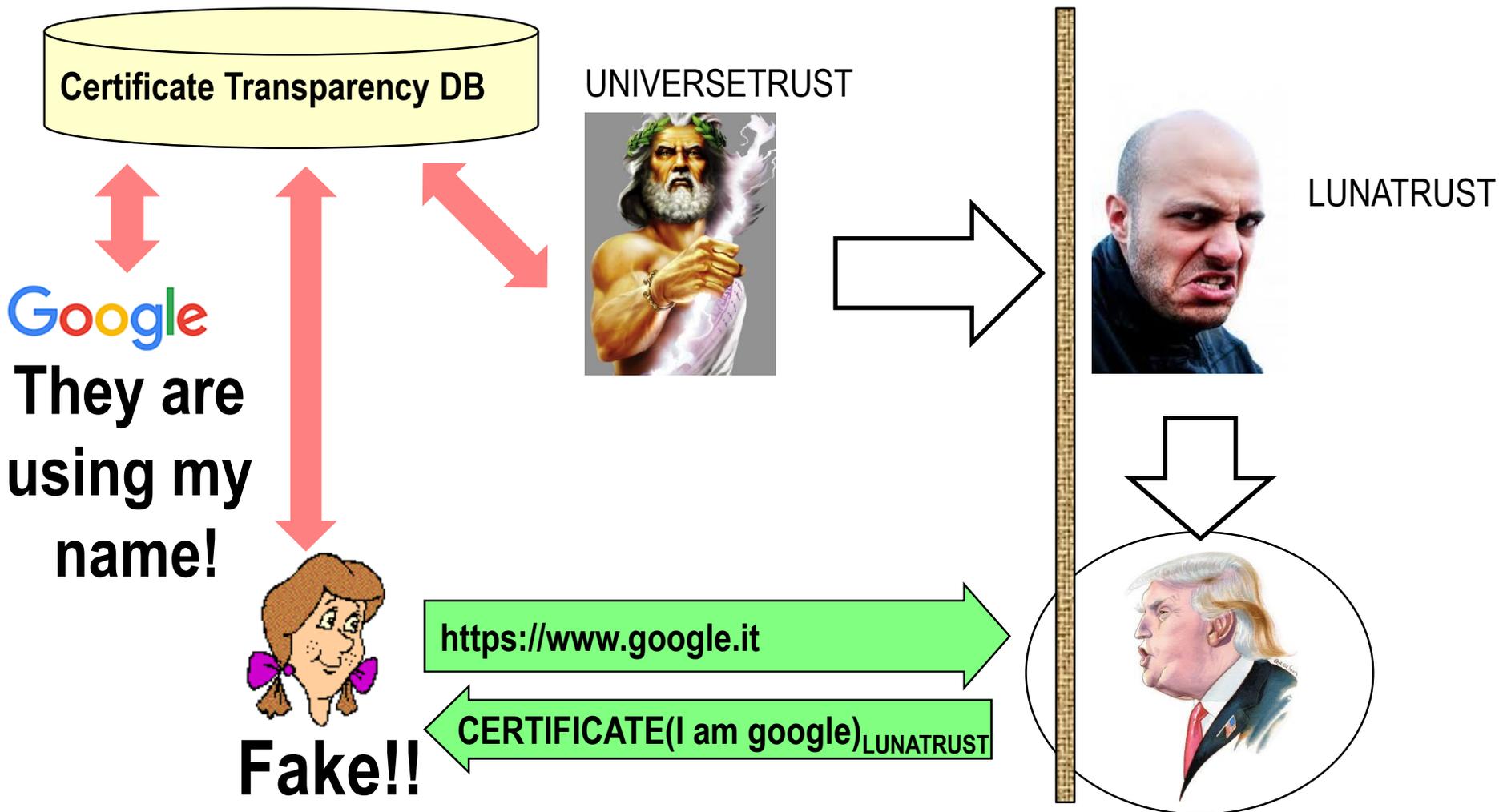
## TLS Proxies: Friend or Foe?

Mark O'Neill, Scott Ruoti, Kent Seamons, Daniel Zappala  
Brigham Young University  
Department of Computer Science  
Provo, UT 84602

Giuseppe Bianchi

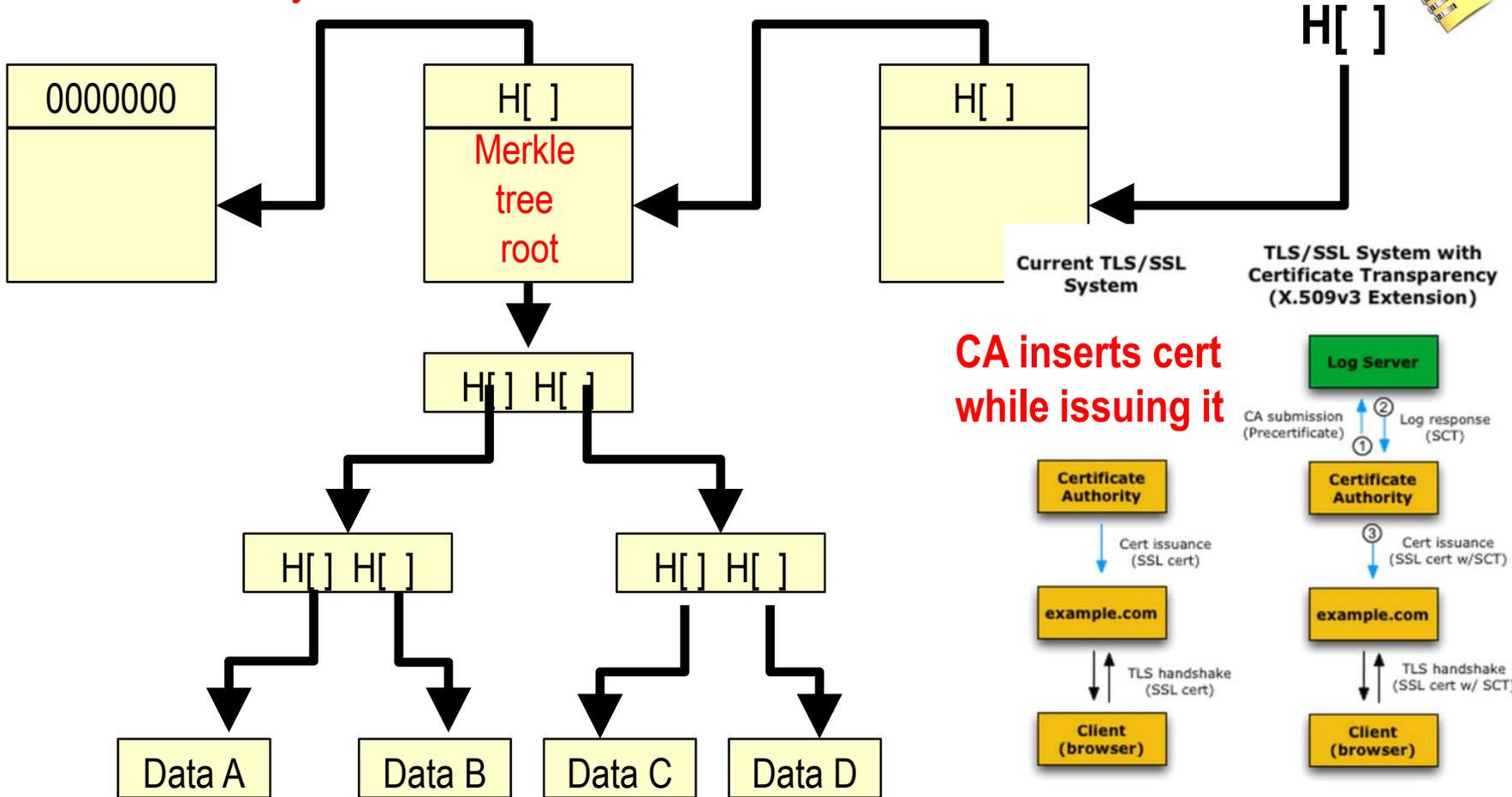
# How to cope with malicious CAs?

Idea: gigantic worldwide DB which anyone can check!



# Done! (2013+, by google+)

1 block every 24 hours

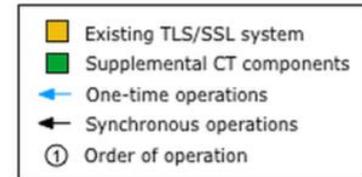


CA inserts cert while issuing it

Fast/easy lookup (merkle tree)

VERY similar to Bitcoin!!

Giuseppe Bianchi



# Blockchain class

## → What they are

⇒ And when you (don't!) need them

## → Basic principles

⇒ Ledger architectures / Consensus / Scripting

## → Which technologies?

⇒ Practice with Multi-chain

## → Which applications?

⇒ Bitcoin

⇒ Multi-signatures

⇒ Lightning network offchain payments

⇒ Crypto currencies and ERC20 ICOs (and fake ones)

⇒ etc