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!

e of unskilled people
etacognitive ability to
y are incompetent
→

being ignorant
ture of ignorance
l world examples!
ol, work, working groups,…

ho are unskilled in these
as conclusions and make
bility to realize it. Across 4
ts of humor, grammar, and
test scores put them in the
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

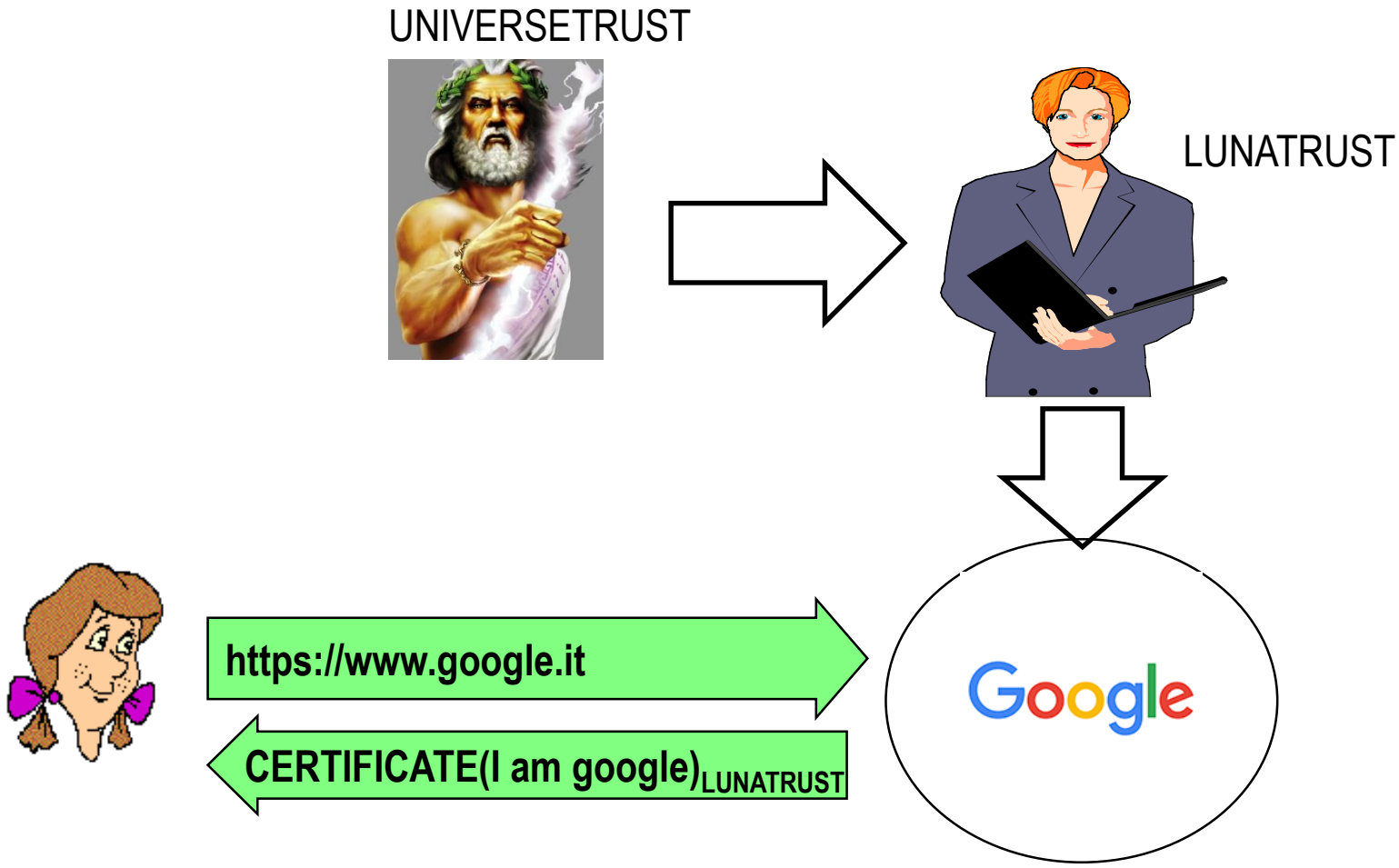
⇨What about data-centric security?
Some very preliminary insights…

Our approach / 3

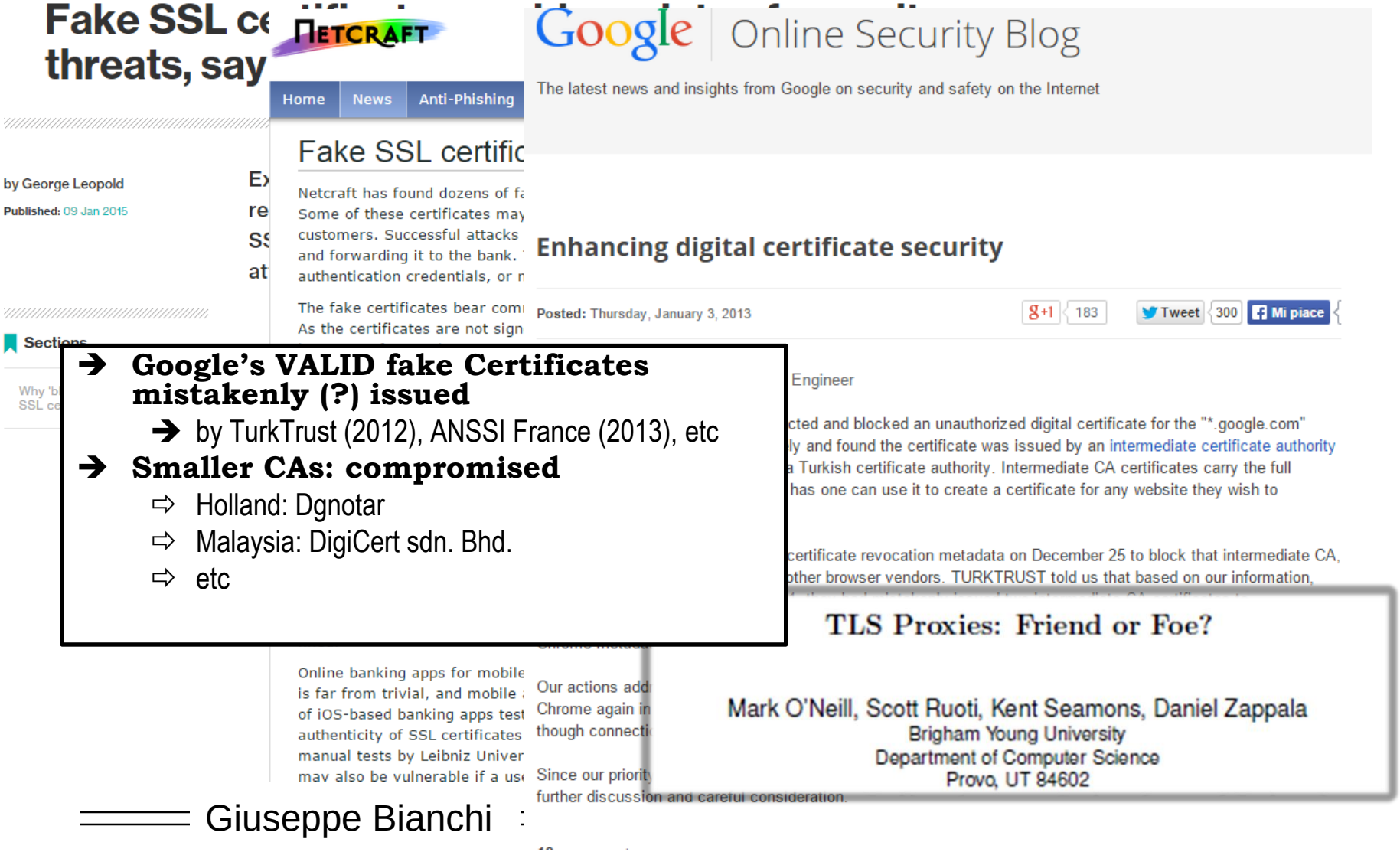
➔Secure storage?

- ⇨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



- ➔ **Google's VALID fake Certificates mistakenly (?) issued**
  - ➔ by TurkTrust (2012), ANSSI France (2013), etc
- ➔ **Smaller CAs: compromised**
  - ⇨ Holland: Dgnotar
  - ⇨ Malaysia: DigiCert sdn. Bhd.
  - ⇨ etc

How to cope with malicious CAs?

Idea: gigantic worldwide DB which anyone can check!

Certificate Transparency DB

UNIVERSETRUST

LUNATRUST

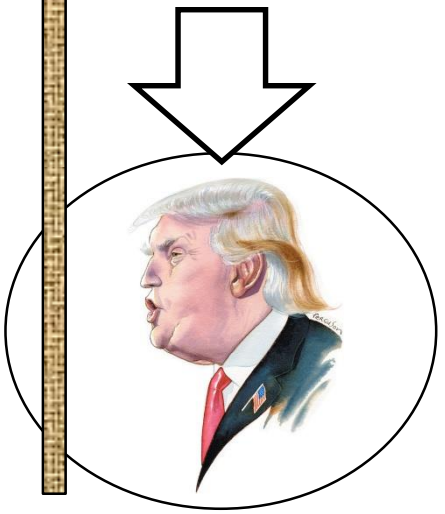
Google

They are using my name!

Fake!!

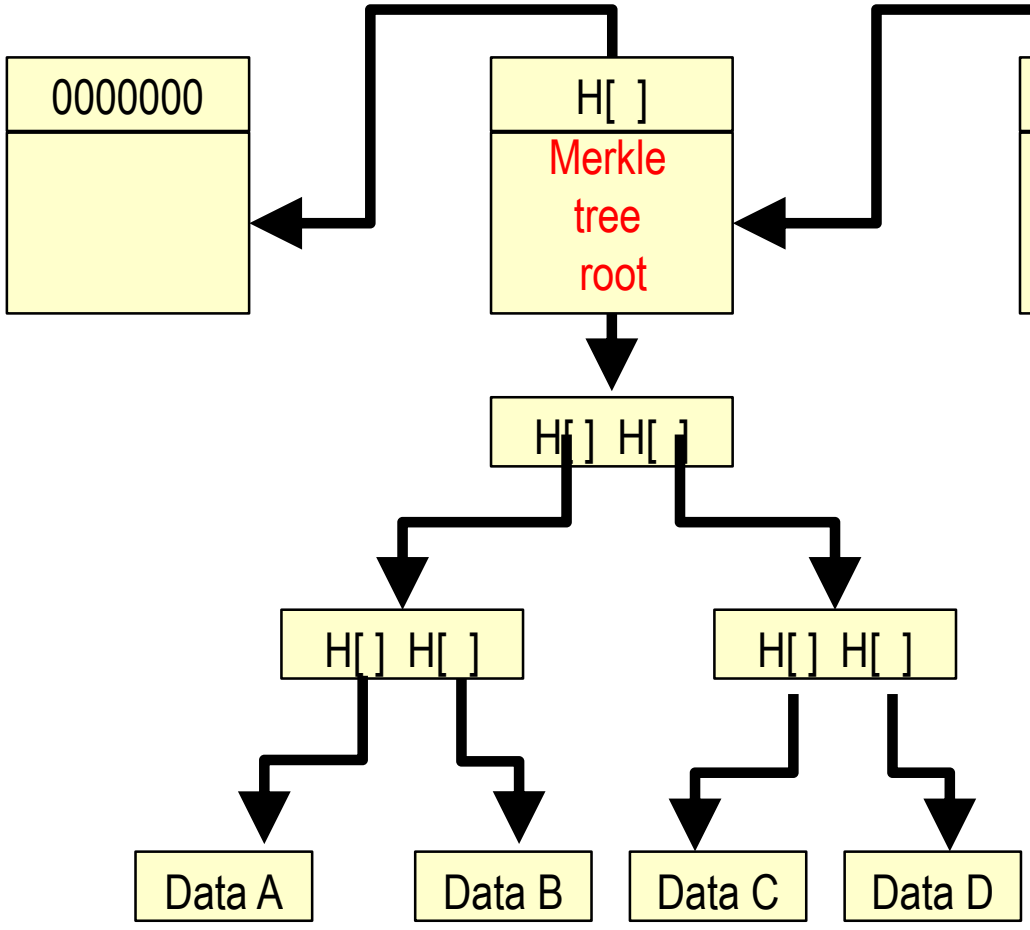
https://www.google.it

CERTIFICATE(I am google)$_{LUNATRUST}$



Done! (2013+, by google+)

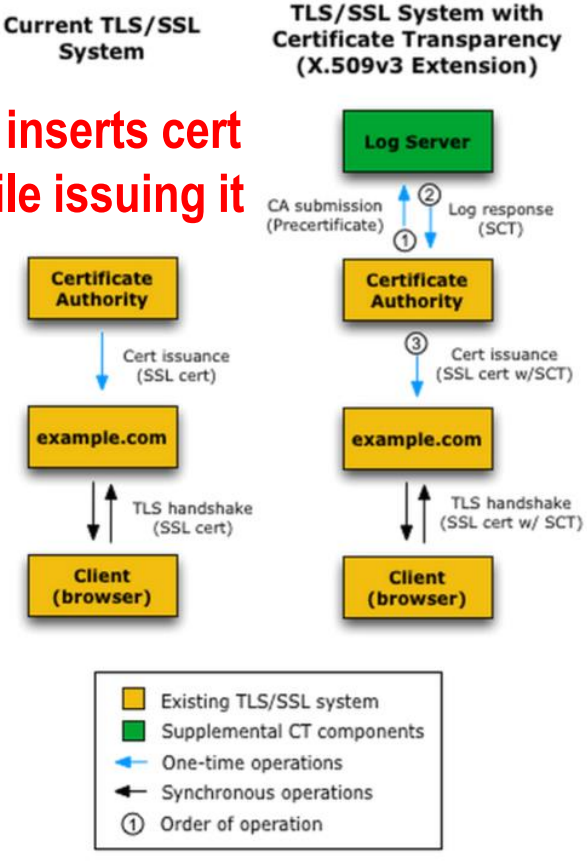
1 block every 24 hours



Fast/easy lookup (merkle tree)

VERY similar to Bitcoin!!

CA inserts cert while issuing it



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