



TFA & Hardware Crypto Tokens

„I know none of my passwords“

OSAK Crypto Party
RWTH Aachen
June 2015

Steffen Vogel
@stv0g
www.noteblok.net





The Cybercrime Economy

2 million Facebook, Gmail and Twitter passwords stolen in massive hack

Frankfurter Rundschau



Frankfurt

Rhein-Main

Politik

Wirtschaft

Panorama

Übersicht | Wissen | Digital | Reise | Gesundheit | Ernährung | Auto | Recht | Karriere

Aktuell: **Schwerpunkt: Liebe** | **Flucht und Zuwanderung** | **Tugce** | **Regionale Startseite**

Digital

Nachrichten aus dem WWW, Tipps zum Computer-Kauf; zu Facebook, iPhone, iPad & Co

06. AUGUST 2014

PASSWORT-DIEBSTAHL

1,2 Milliarden Passwörter erbeutet

Von CHRISTOPH DERNBACH



ONLINE
FOCUS



Übersicht



Ressorts



Suche

INTERNET

Google bestätigt Passwort-Klau indirekt **Zugangsdaten zu 5 Millionen Gmail-Konten veröffentlicht**

Donnerstag, 11.09.2014, 08:45

TECHNOLOGY

Russian Hackers Amass Over a Billion Internet Passwords

By **NICOLE PERLROTH** and **DAVID GELLES** AUG. 5, 2014



JUST IN [HOW TO TURN YOUR WINDOWS 10 UPGRADE FILES INTO AN ISO DISK IMAGE](#)

Dropbox blames other services for claimed 7 million password hack

This is your regularly scheduled reminder to turn on two-factor authentication where available.

Two-Factor-Authentication (TFA)

Make sniffed passwords useless

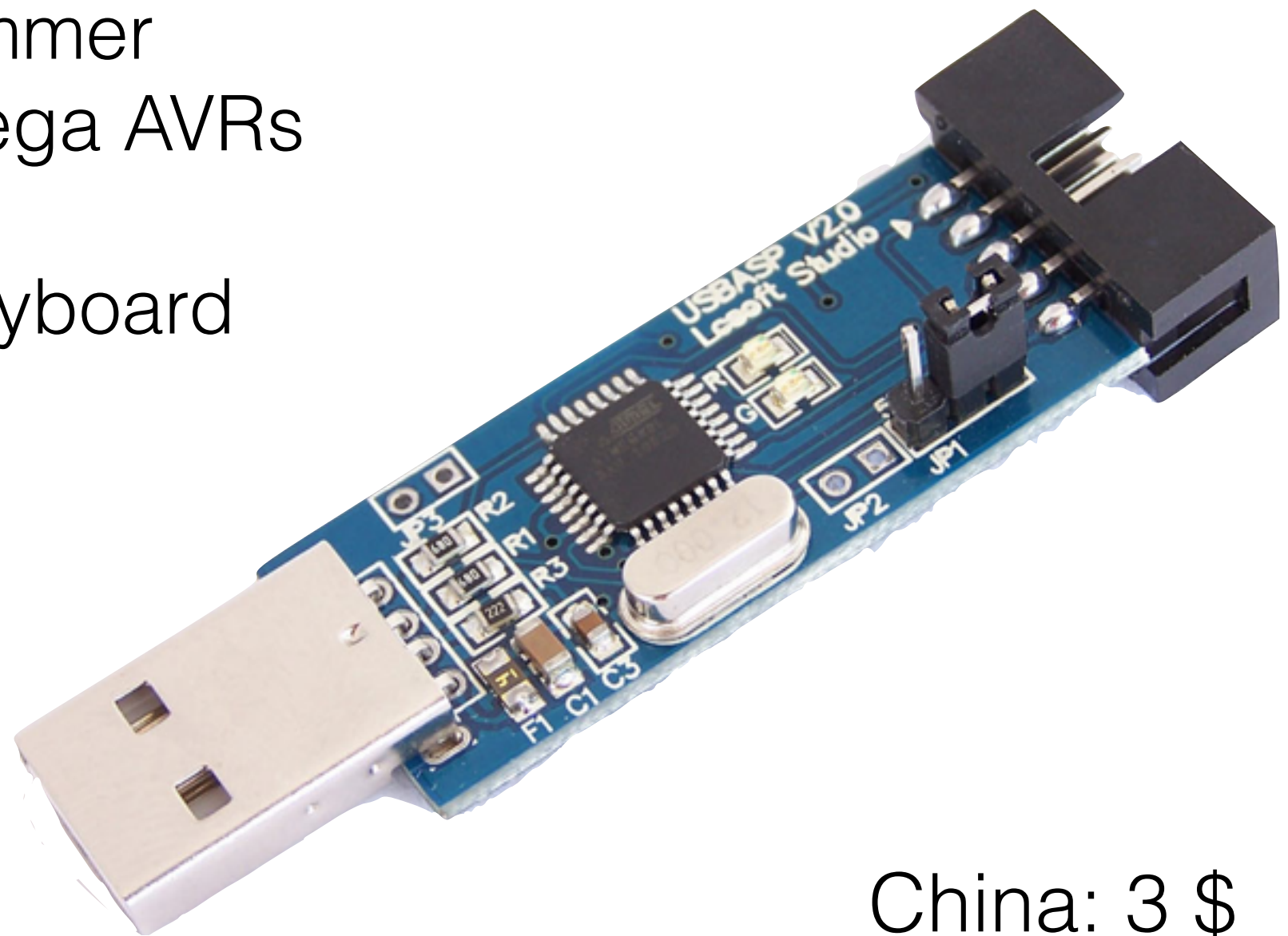
- Password **and** Pin-Code required for authentication
- Code is:
 - generated by: SMS, App, Token, TAN list
 - only valid once, for a limited time
- Similar to One-time passwords (OTP)
- Well-established practice for online banking (TAN)

Hardware Token

my first steps...

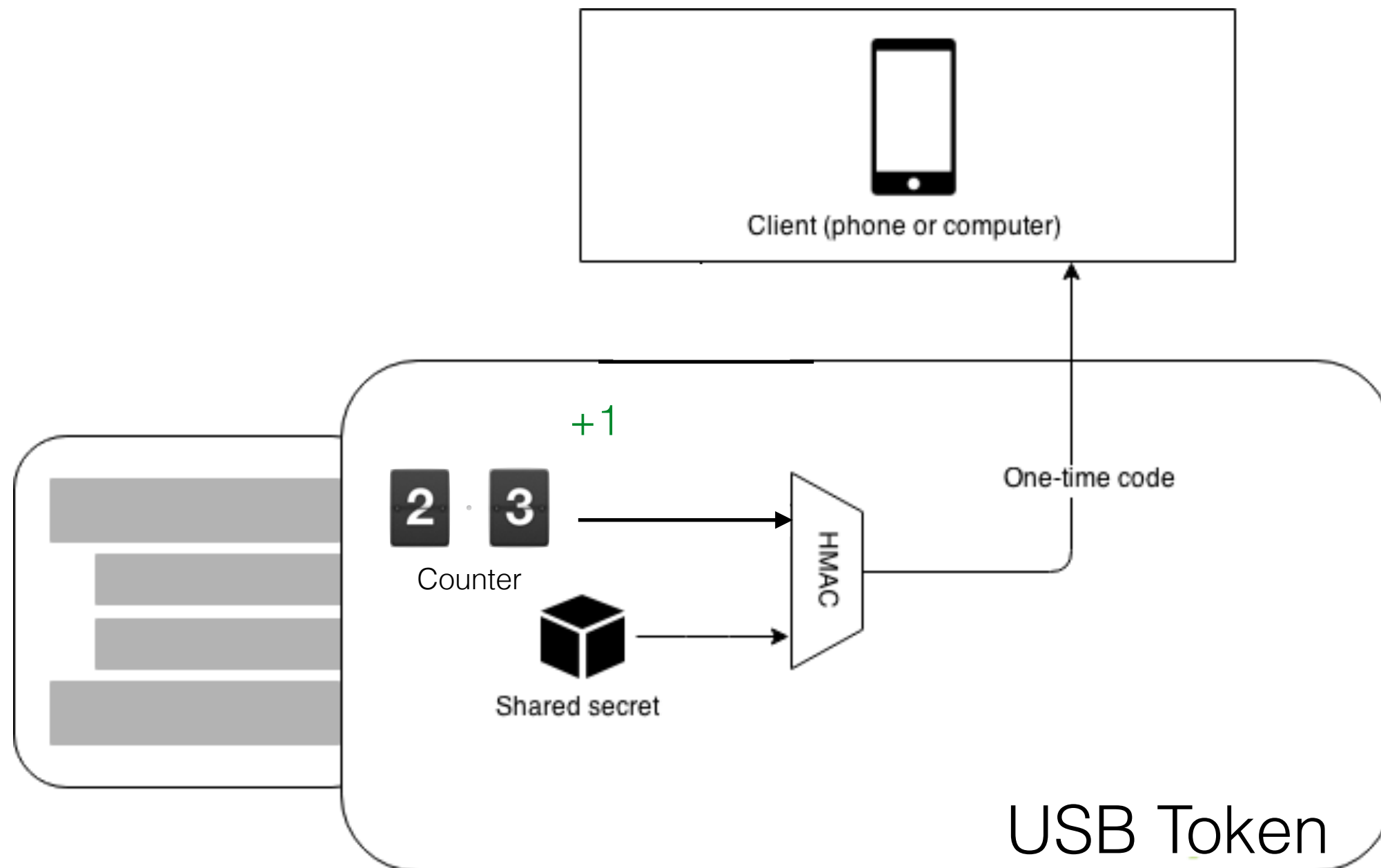
USBasp Programmer
for Atmel ATmega AVR

emulates HID keyboard



China: 3 \$

OTP Generation on Tokens

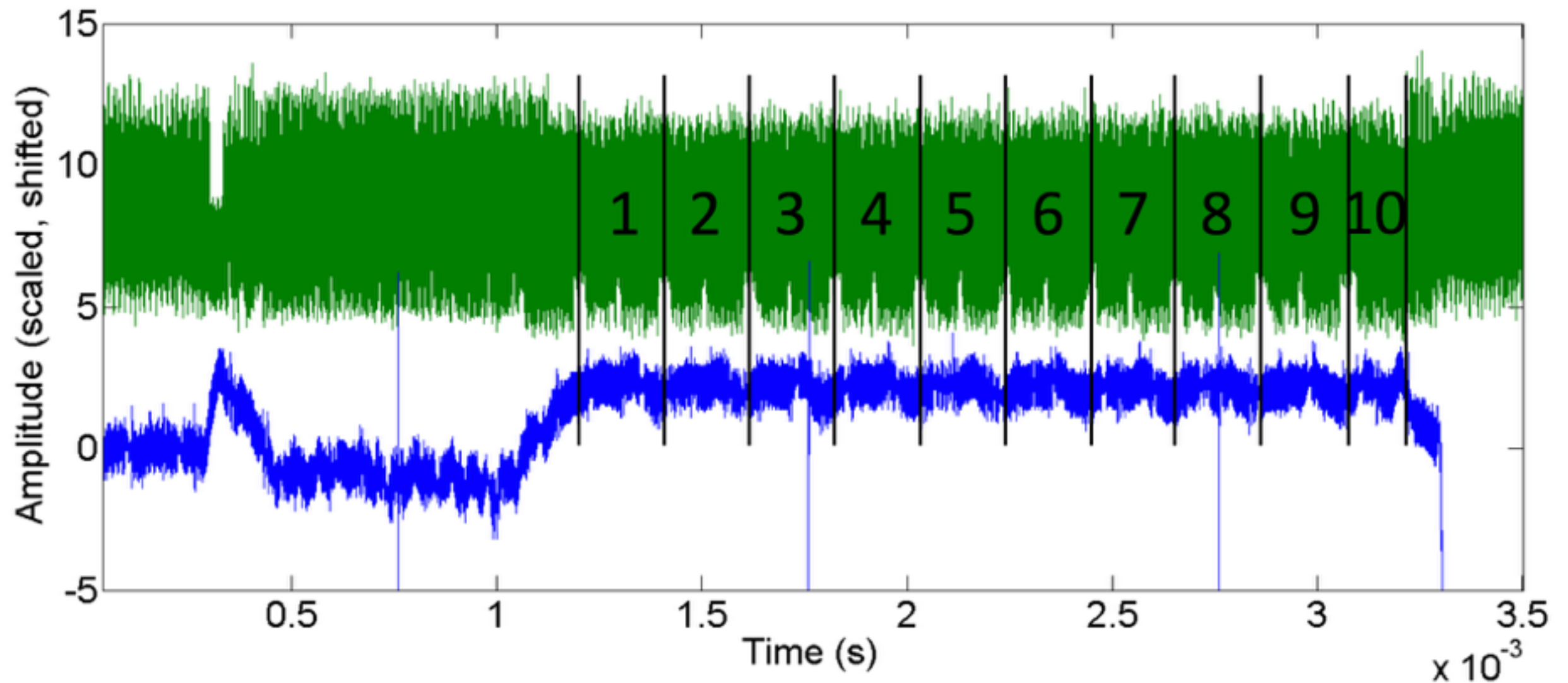
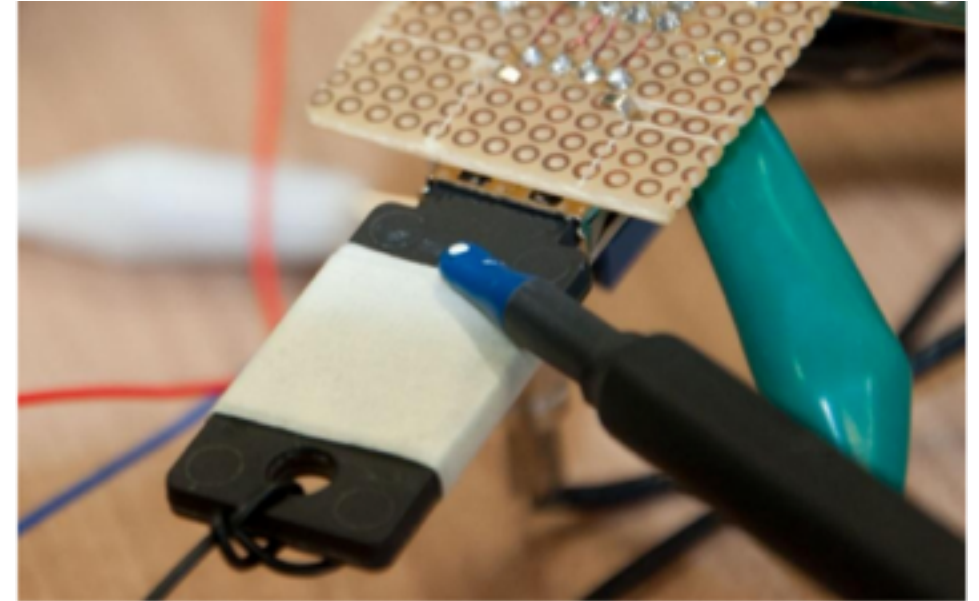


Challenge Response

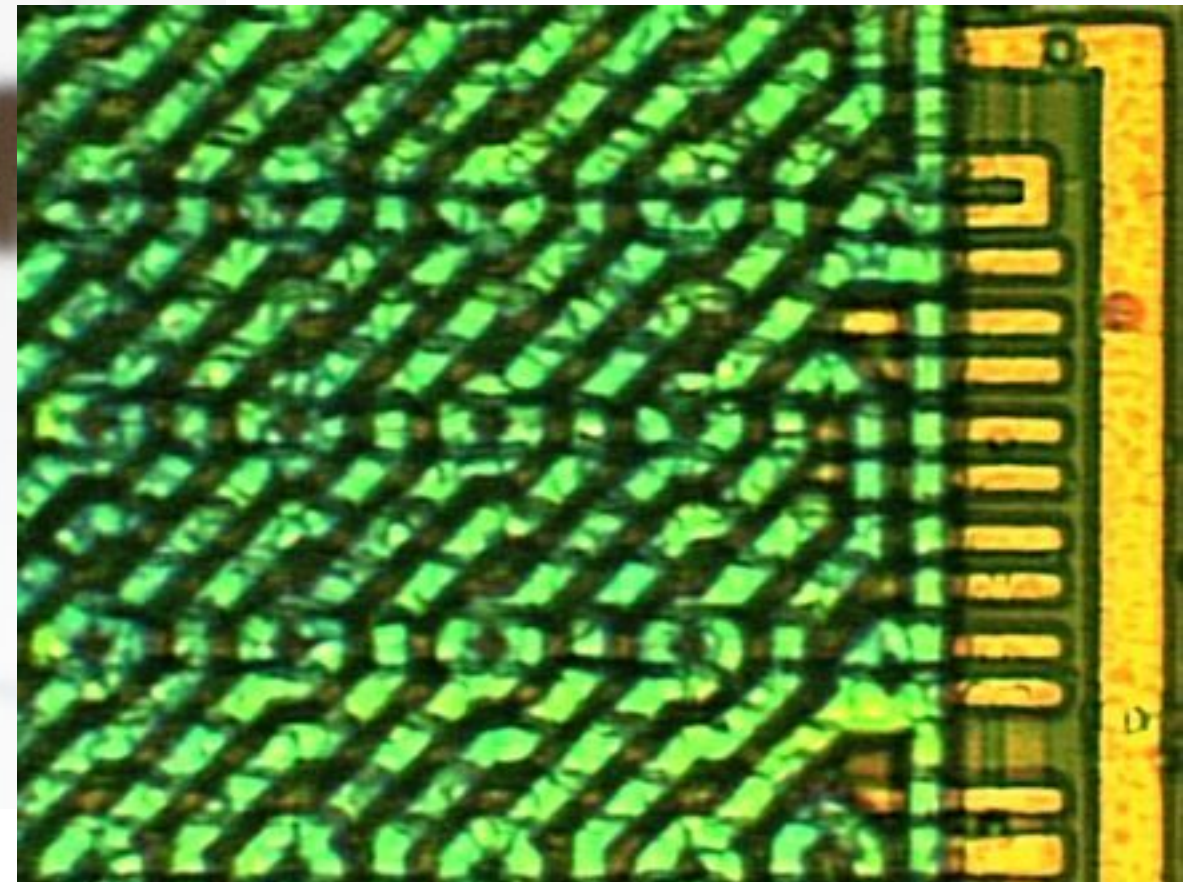
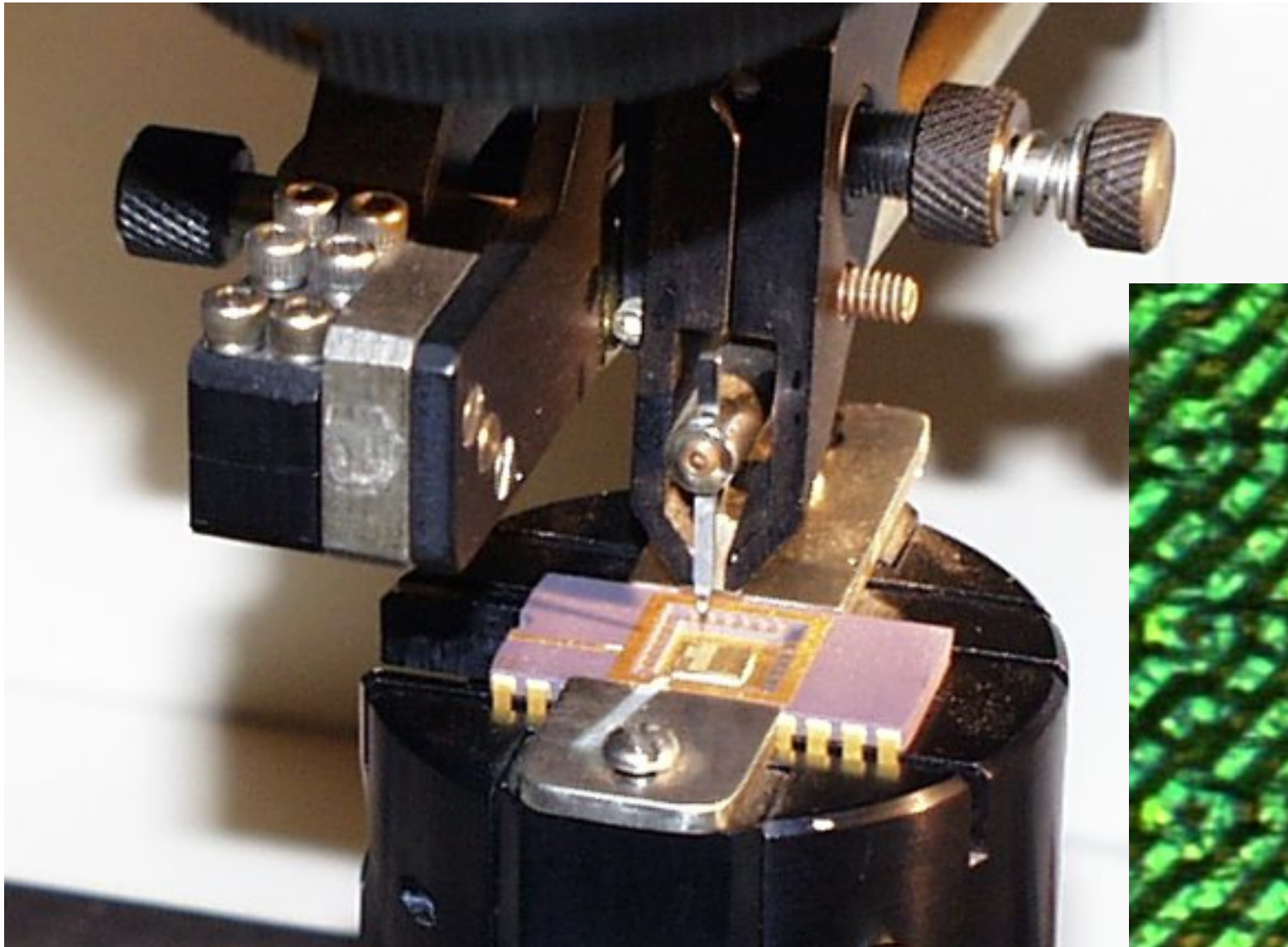


Side channels attacks

From:
Extracting keys from FPGAs, OTP Tokens
and Door Locks, David Oswald, 30C3



Shielding & Probing



https://www.usenix.org/legacy/events/smartcard99/full_papers/kommerling/kommerling_html/

Smart Cards

Protect your most sensitive information in a safe where it's impossible to extract them.

- Login Credentials
- Private Keys



! Decryption / token generation is inside done inside the smart card.

Smart Cards

- Applications: SIM, eID, BlueCard, Credit Cards, etc.
- Hardened secure crypto processors:
 - Side channels: EMF, timing, current consumption
 - Tampering: Probing, Decaps, Die Shots
- Operating systems: JCOP & MULTOS
 - Can run arbitrary Java applets
- Mostly closed source due to NDA's 🤨





plug-up Key

- Cheap: 6 €
- U2F only token

FIDO U2F

- Challenge Response Authentication
- Supported by:
 - Google, PAM, Wordpress
 - Chrome (JS API)
 - Fido Consortium





OpenPGP Smartcard

- 3 independent 2048 bit RSA keys
- Protection by PIN / PUK
- Smart card reader required!
- Nice integration with GnuPG
- FSF Fellowship card



ID Bridge K30

- CCID compatible smart card reader
- Can be used with OpenPGP smart card





NitroKey

former GPF Crypto Stick

- Combines:
 - OpenPGP Smart Card
 - uSD slot for encrypted storage
- Open Source
- Not yet available
- Expensive: ~60 €





Yubikeys

- Swiss army knife of tokens
- Applications for:
 - OpenPGP, U2F, OTPs
 - OATH-{H,T}OTP
 - Challenge Response
- Interfaces: USB (HID, CCID) & NFC (NDEF + ...)
- Price tag: 18 - 50 €



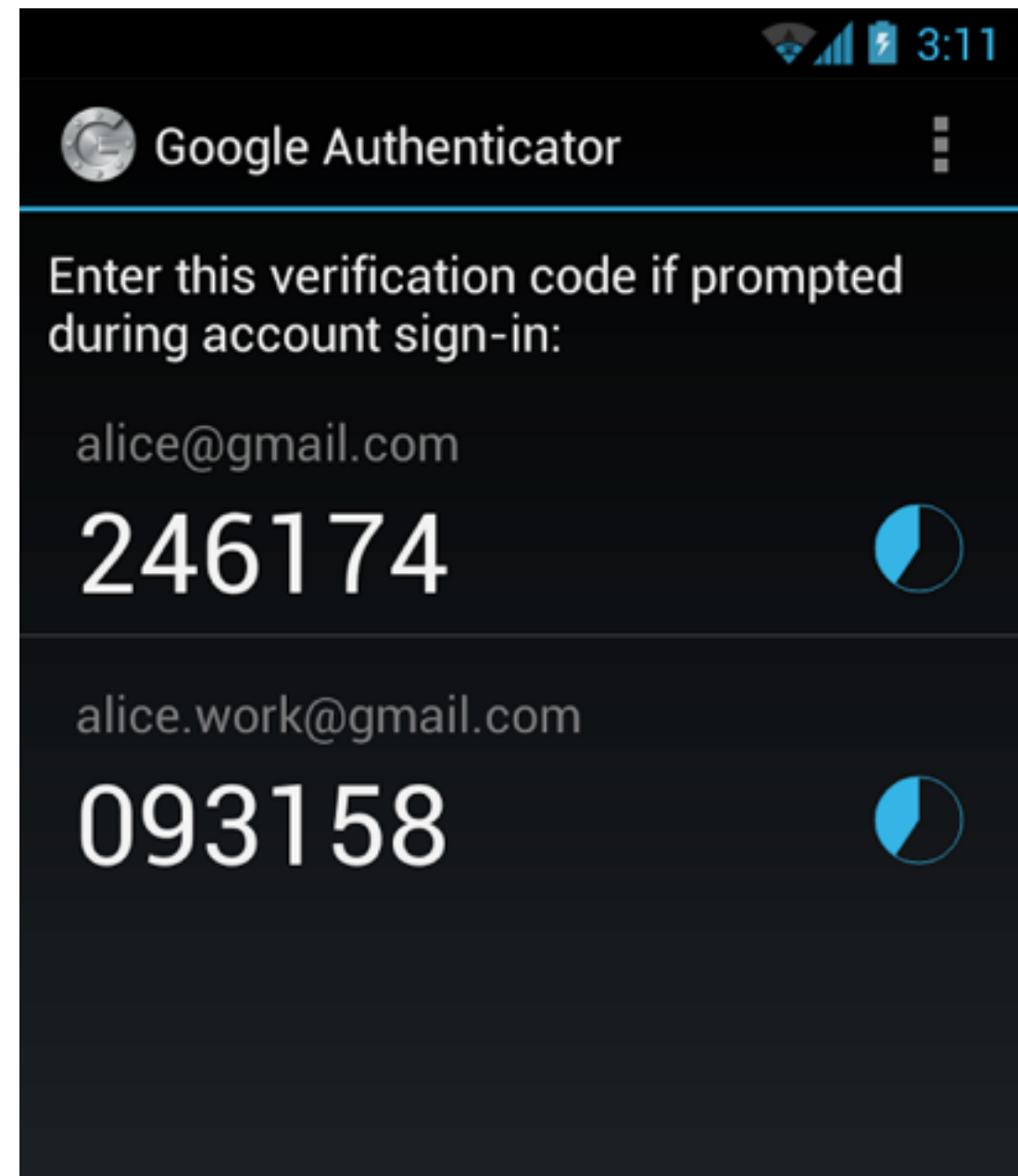
Software

- Increased security destroys user experience!
- Major obstacle is integration!
 - across various OS's
 - multi homing: desktop, notebook, phone



{Yubico, Google} Authenticator

- Implements OATH-TOTP in an Android App
- Most common TFA App
- Yubico fork stores private keys on token





GnuPG

The OpenPGP smart card stores up to three private keys (RSA 2048 bit) on a token.

Decryption / signing is protected by PIN's

The public part of the key is not stored on the token!

1. `gnupg --card-status`
2. `gnupg --edit-card`

DEMO



{ssh,gpg}-agent

Use your token to login to remote machines:

1. Start with SSH support:
`gpg-agent --enable-ssh-support`
2. Show available GPG keys:
`ssh-add -L`
3. Add key to `~/.ssh/authorized_keys`

DEMO



Pluggable Authentication Modules (PAM)

- PAM Modules available for:
 - OATH-{H,T}OTP
 - U2F
 - Yubikey Challenge Response
- Remote Challenge Response (via SSH) is tricky

DEMO



password-store

- Unix-style password manager
- Based on: GnuPG, Git, Xclip, Bash
- Open and simple data format
- No „cloud“
- Easy integration: Ansible, Android, Firefox, etc..

DEMO

More integration....



KeePass



~~LastPass~~



OpenKeyChain

My Recommendations

1. Enable TFA wherever supported:
<https://twofactorauth.org>
2. Get a Hardware Token:
<https://yubico.com> <http://dongleauth.info>
3. Use a tool to manager your credentials:
<http://passwordstore.org>
4. Replace cloud by self-hosted services:
<https://prism-break.org>

Thank you

Slides: www.noteblok.net

Contact: stv0g@0l.de

3AF4 0556 6D86 9684 99E5 3D5B 04EC 8518 B35D 3BE5