

Over-the-Air Cross-platform Infection for Breaking mTAN-based Online Banking Authentication

Alexandra Dmitrienko
Fraunhofer Institute for Secure
Information Technology/CASED, Germany

Joint work with

Lucas Davi
TU Darmstadt/CASED

Ahmad-Reza Sadeghi
Fraunhofer SIT
TU Darmstadt/CASED

Christopher Liebchen
TU Darmstadt /CASED

Online Banking

- Widely used overall the world
- Convenient for users
- Cheap for banks (low per-transaction costs)
- Unfortunately, also good for attackers
 - Attacks can be automated and hence scale well

Online Banking Security Trends

- Cat and mouse games (banks vs. attackers)
 - Attacks are becoming more sophisticated and real
 - Banks address new threats by adapting new authentication schemes
- Current trend for solutions
 - Two-factor authentication

Two-Factor Authentication Schemes

- Use two authentication tokens (T1 & T2)
- Various solutions exist (based on extra devices, or hardware tokens, mobile phones, etc.)
- Solutions involving mobile phones as one factor seem to be very convenient and trendy

one-time
password or a
cryptographic
secret

T2



Typically login
credentials

T1



Two-factor Authentication Schemes with Mobile Phones

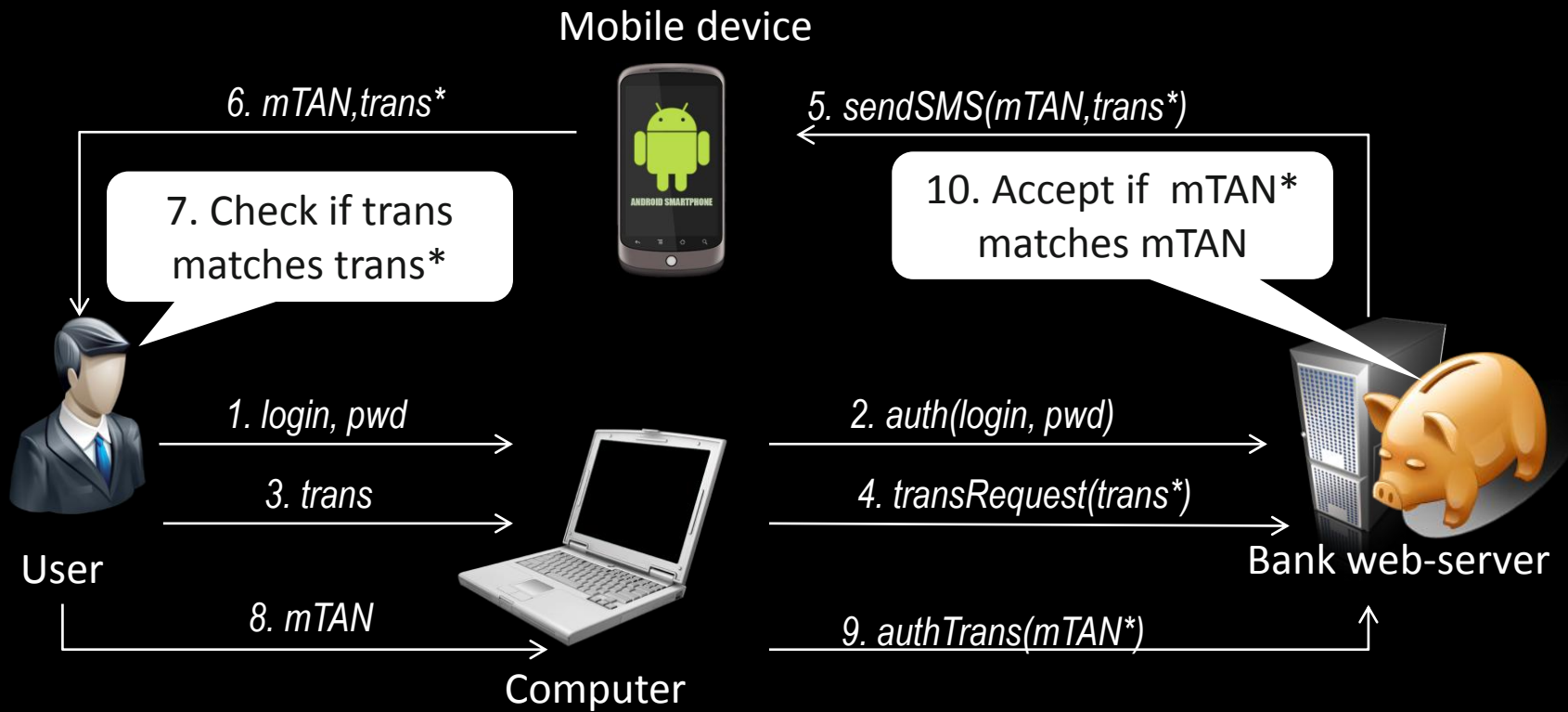
mTAN Authentication

photoTAN Authentication

Transaction Signatures

others...

mTAN Authentication



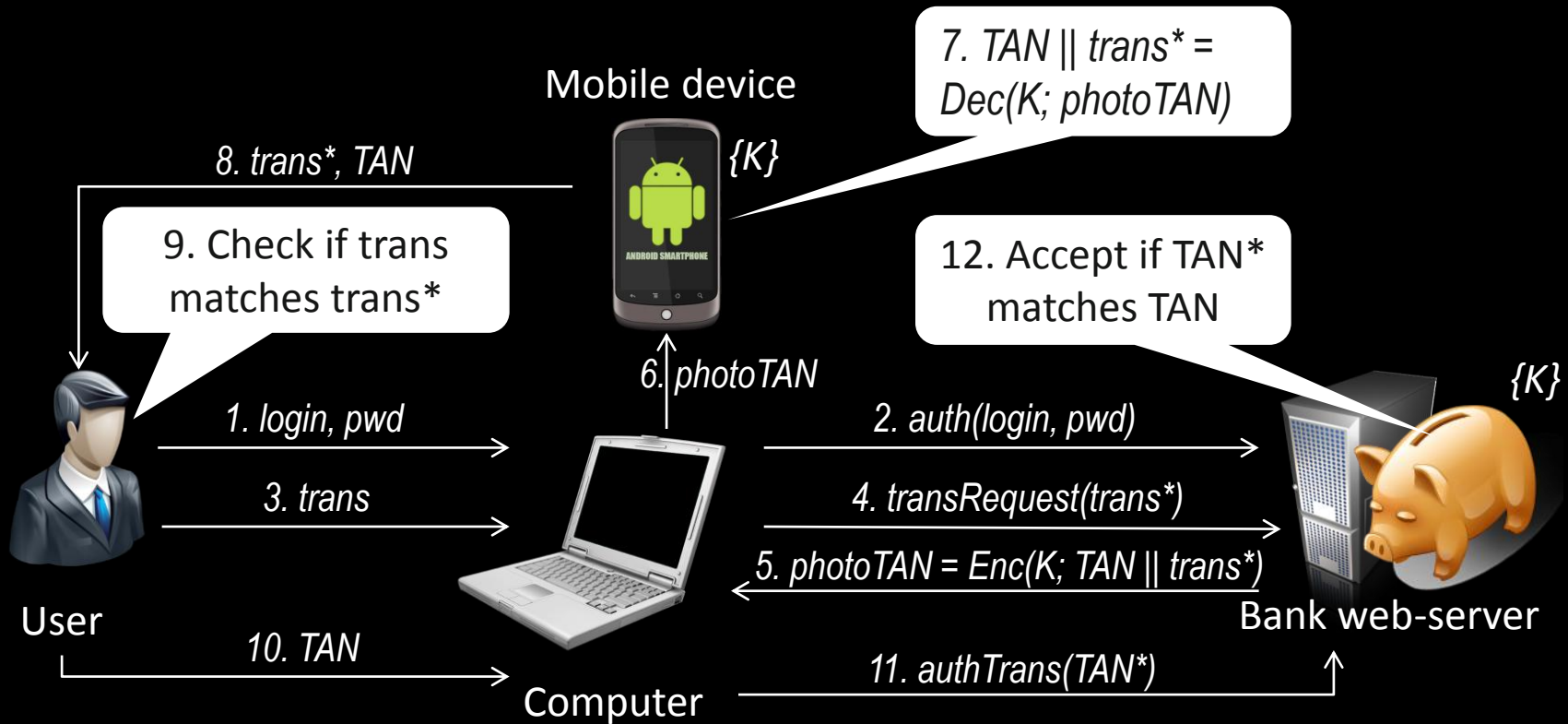
T1

Login, pwd

T2

Mobile Transaction Authentication Number (mTAN)

photoTAN Authentication



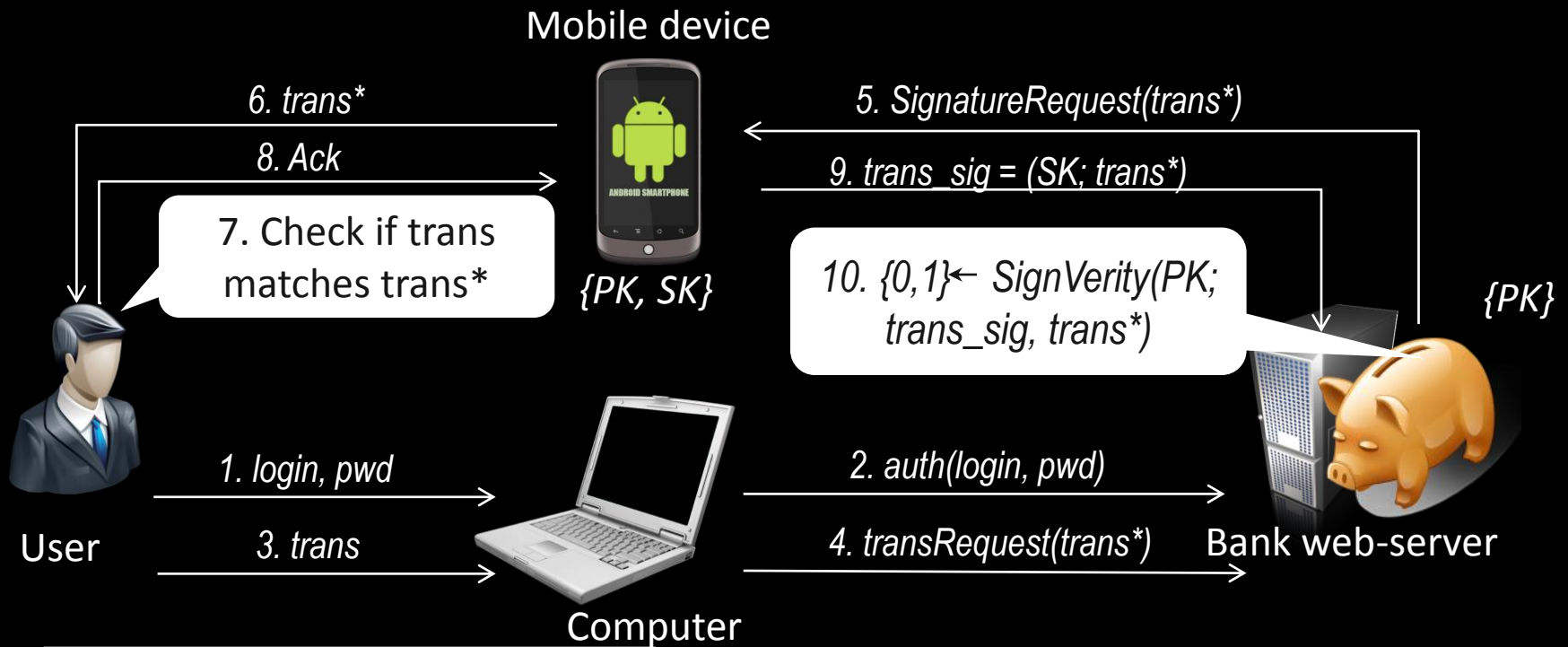
T1

Login, pwd

T2

K – a key shared by the mobile device and the bank

Authentication with Transaction Signatures



- T1 Login, pwd
- T2 SK – client private key

mTAN Scheme: Widely Spread

European banks:

- Austria, Bulgaria, Germany, Hungary, the Netherlands, Poland, Russia, South Africa, Spain, Switzerland and some in New Zealand and Ukraine

American banks:

- Provided optionally
- E.g., SafePass by Bank of America, the bank with more than 20 million of active online banking users

China:

- Provided optionally
- E.g., SMS verification scheme by ICBC, the largest Chinese commercial bank with more than 100 million of customers using online banking

Known Attacks on mTAN Scheme

SIM Swap Fraud attack [4]

- Attacker obtains a replacement SIM for the victim's phone
- Attacker must spoof identity of the victim (e.g., show passport)
- The attack can target some specific customers

Malicious network operator [5]

- Attacks by insiders from telecommunication providers
- Attack breaks assumption on trustworthy network operator


Online banking malware

- Coupled host/mobile malware (e.g., ZeuS/ZitMo and SpyEye/Spitmo)
- Targets are Android, Windows Mobile, BlackBerry, Symbian

News

Zeus Banking Trojan Hits Android Phones

Zeus crimeware creators adapt Zitmo malware, disguised as a banking activation application, to steal financial details from Android users.

By **Mathew J. Schwartz**  InformationWeek
July 13, 2011 06:47 PM

The Trojan spyware application known as Zitmo, which is designed to steal people's financial data, has now been altered to target devices running the Android mobile operating system.

"The malware poses as a banking activation application," said Axelle Aprville, a senior antivirus analyst and researcher for Fortinet, in a [blog post](#). "In the background, it listens to all incoming SMS messages and forwards them to a remote web server."



(click image for larger view)

Slideshow: 10 Massive Security Breaches

More Security Insights

Webcasts

- [How not to go Dark on Black Friday](#)
- [Delivering on Real-time and Cross-](#)

That's a security risk, as some banks now send mTANs--mobile transaction authentication numbers, which is banking-speak for one-time passwords for authenticating transactions--via SMS. By intercepting these passwords, [the Zeus-botnet-using criminal gang](#) behind Zitmo can not only create fraudulent money transfers, but verify them.

News

BlackBerry, Android users targeted by new Zeus trojan

Dan Kaplan August 08, 2012

 PRINT  EMAIL  REPRINT  PERMISSIONS TEXT: [A](#) | [A](#) | [A](#)

 Twe

Kaspersky Lab researchers say they have detected five new variants of a mobile trojan known as ZitMo, and four of them target BlackBerry devices, which typically have gone untouched by hackers

ZitMo, which stands for "Zeus in the mobile," **first appeared** roughly two years ago. It is designed to steal mobile transaction authentication numbers (mTANs), or one-time passwords, that some banks, mostly in Europe, send via SMS message to mobile users as an additional layer of security.

RELAT

- Zeu
ban
- Zeu
snif

MORE

- Mic
on F

News

Malware & Viruses

New 'Spitmo' Banking Trojan Attacks Android Users

Matt Liebowitz, SecurityNewsDaily Staff Writer
September 13 2011 06:03 PM ET



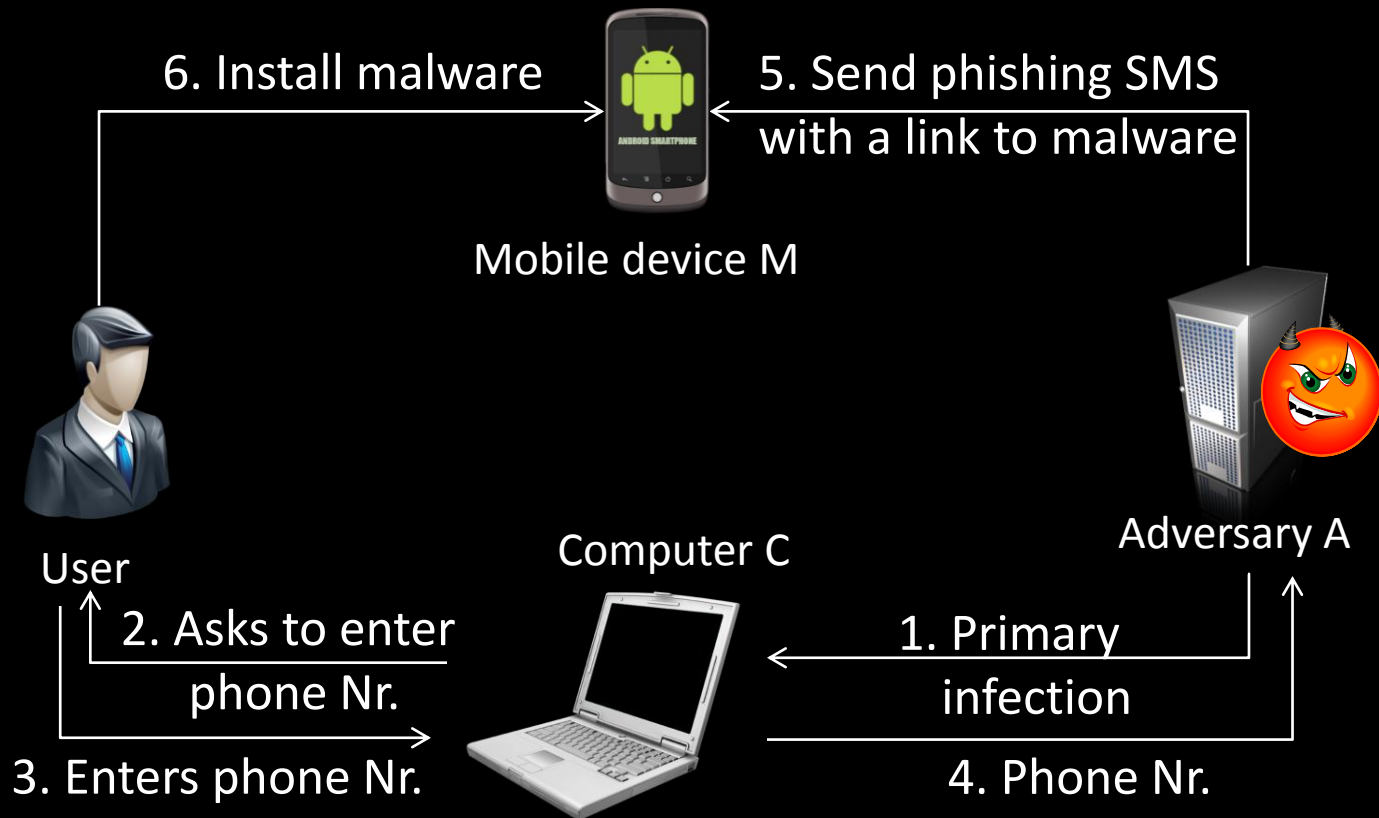
Online crooks have reworked a notoriously devious bank-account-stealing Trojan to target Android smartphone customers.

Called Spitmo (SpyEye in the mobile browser), the nasty software first infects a PC's Web browser, then rigs a targeted bank's login page with a fake security warning that "pretends to be an Android application designed to protect the phone's SMS messages from being intercepted (there's irony for you...)" and will protect the

user against fraud," the security firm Trusteer [wrote](#).

Spitmo also prompts mobile customers to enter their cellphone number and their device's international mobile equipment identity (IMEI) number, which is unique to each handset.

ZeuS/ZitMo: Attack Scenario to Compromise End-Points



Shortcomings of Existing Online Banking Malware

- A lot of user interaction
 - Phishing to obtain user phone number
 - Phishing do lure the user to install malware
- Users are warned not to fall into phishing trap
 - By banks (on web-cites)
 - By police (reports)
 - Legal authorities (e.g., by German Central Board of Credit Institution)

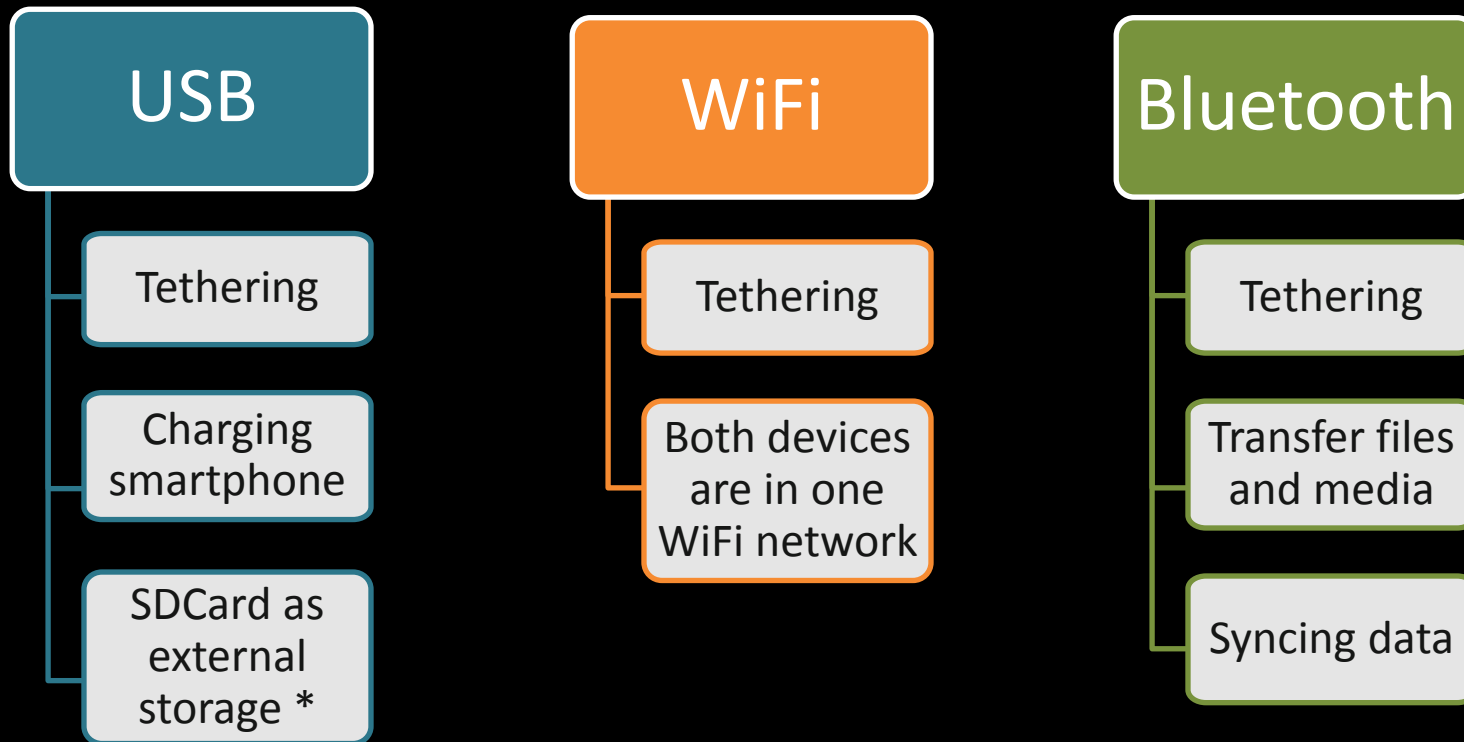
=> Can it get worse? More stealthy?

Our Contribution

- Cross-platform infection in context of online banking attacks and attacks against two-factor authentication
 - Allows the attacker to take control over user's PC and the mobile phone
 - Establishes pairing between user's PC and the mobile phone involved in the same authentication session
 - Requires no (or minimal) user interaction

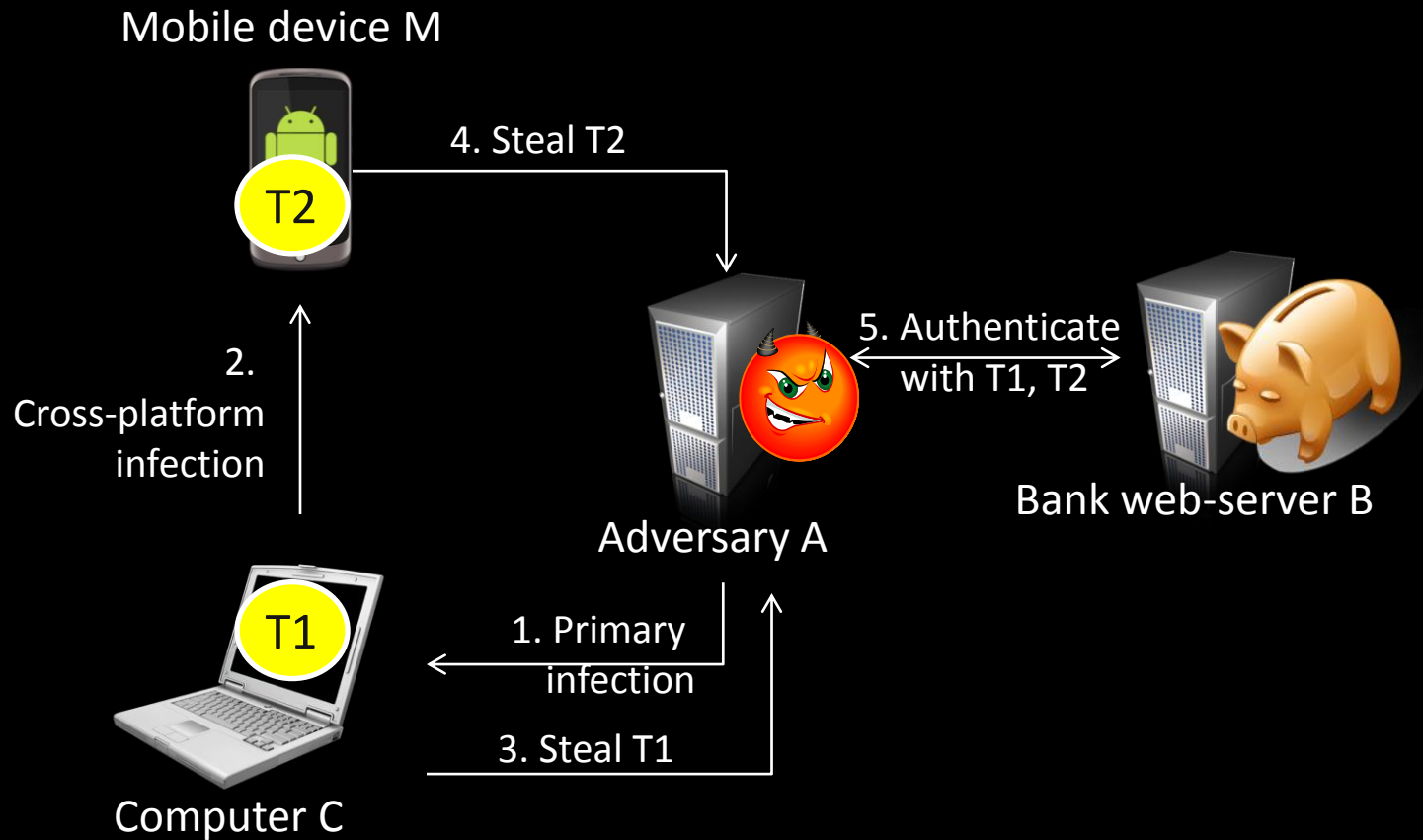
Cross-Platform Infection

- As soon as PC and the mobile device get connected



* Cross-device infection over USB has been shown by Stavrou et. al at BlackHat DC 2011 [2]

Cross-Platform Infection for Bypassing Two-Factor Authentication using Mobile Devices



Our Attack Instantiation

- Attack against mTAN authentication
- Primary infected device is the PC
- Cross-platform infection
 - when PC and the mobile device/phone are connected to the same WiFi network
- Our target platforms
 - PC: Windows 7 (Firefox web-browser)
 - Mobile device: Android 2.2.1

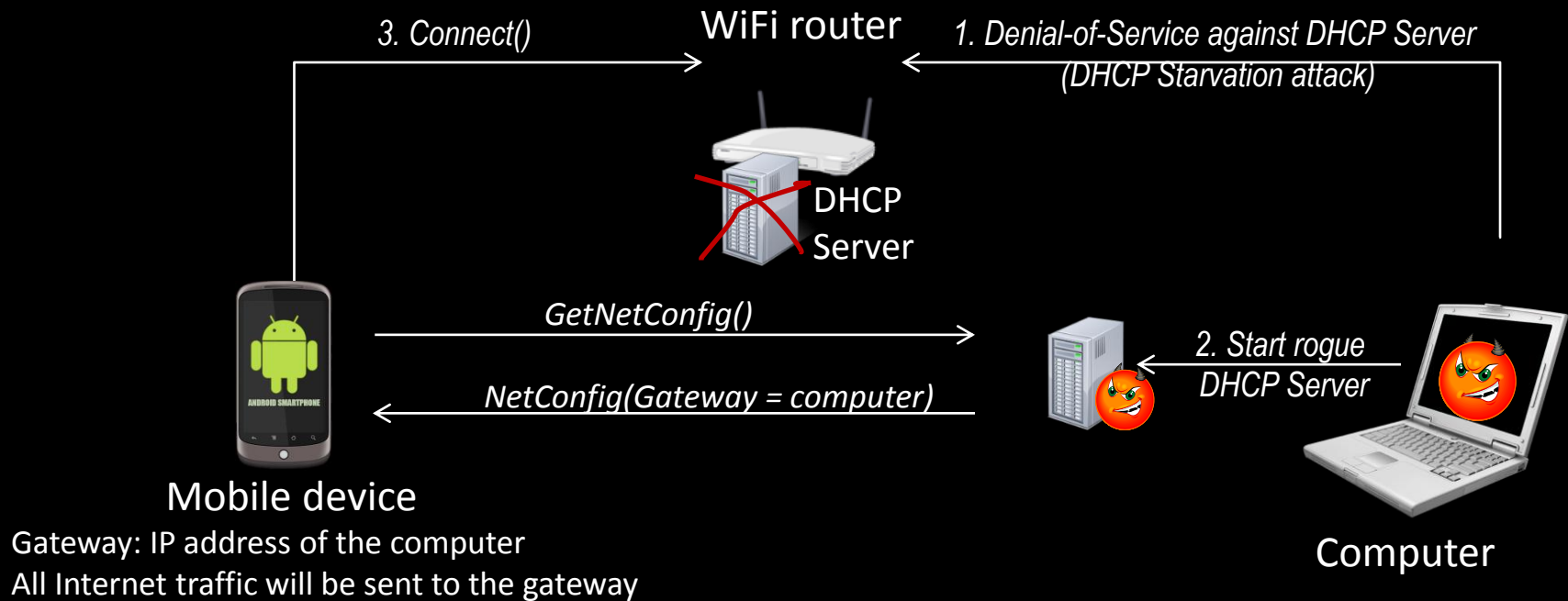
Step 1: Primary Infection

- PC is compromised
 - Reasonable and basic assumption (PC malware is widely spread)
 - Could be done by means of PC-to-PC cross-device infection
 - Two-factor authentication is meant to tolerate malicious PCs

Step 2: Cross-Platform Infection

Phase 1: Man-in-the Middle Attack in WiFi Network

- DHCP Starvation attack + rogue DHCP server to become a man in the middle

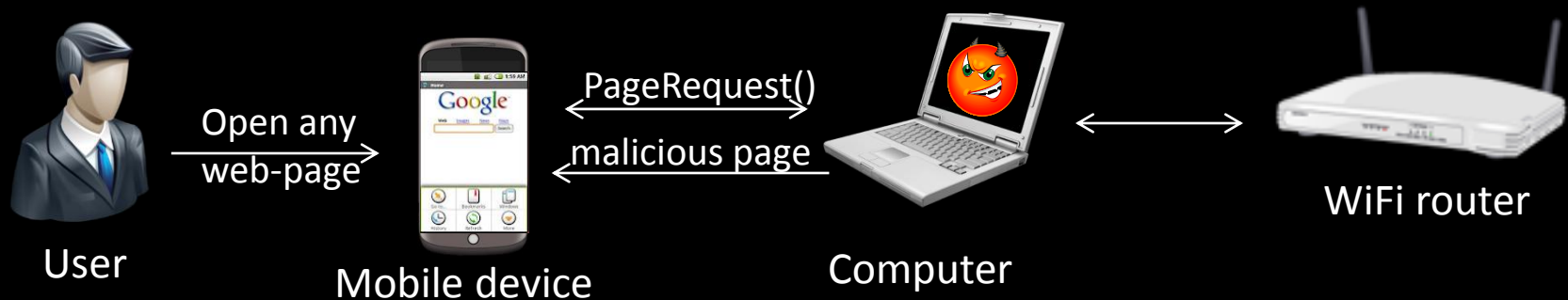


- Other techniques can be used to become a man-in-the middle (e.g., ARP cache poisoning)

Step 2: Cross-Platform Infection

Phase 2. Page Substitution

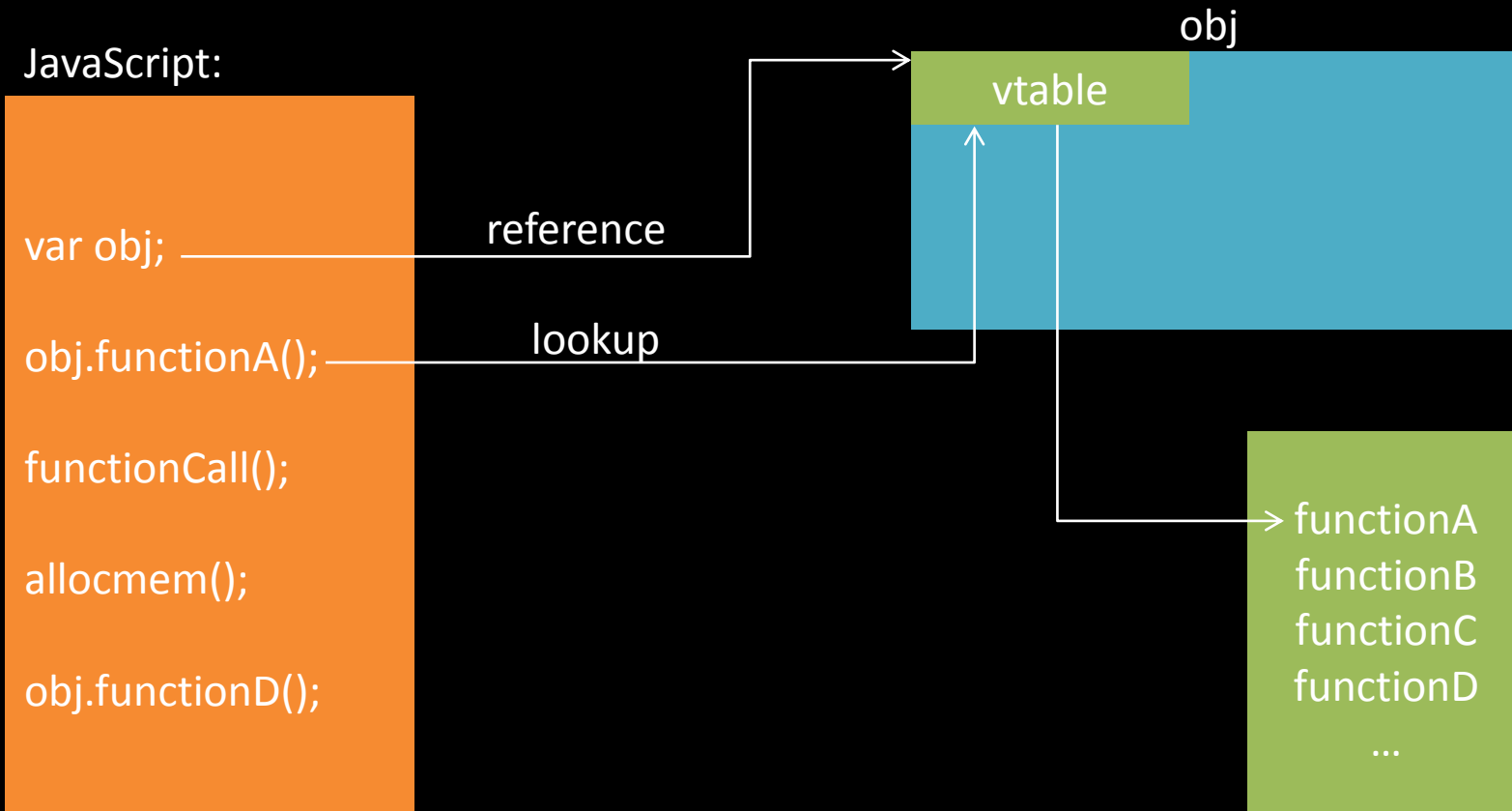
- Malicious gateway substitutes the requested page with a malicious one



Step 2: Cross-Platform Infection

Phase 3: Remote Exploitation

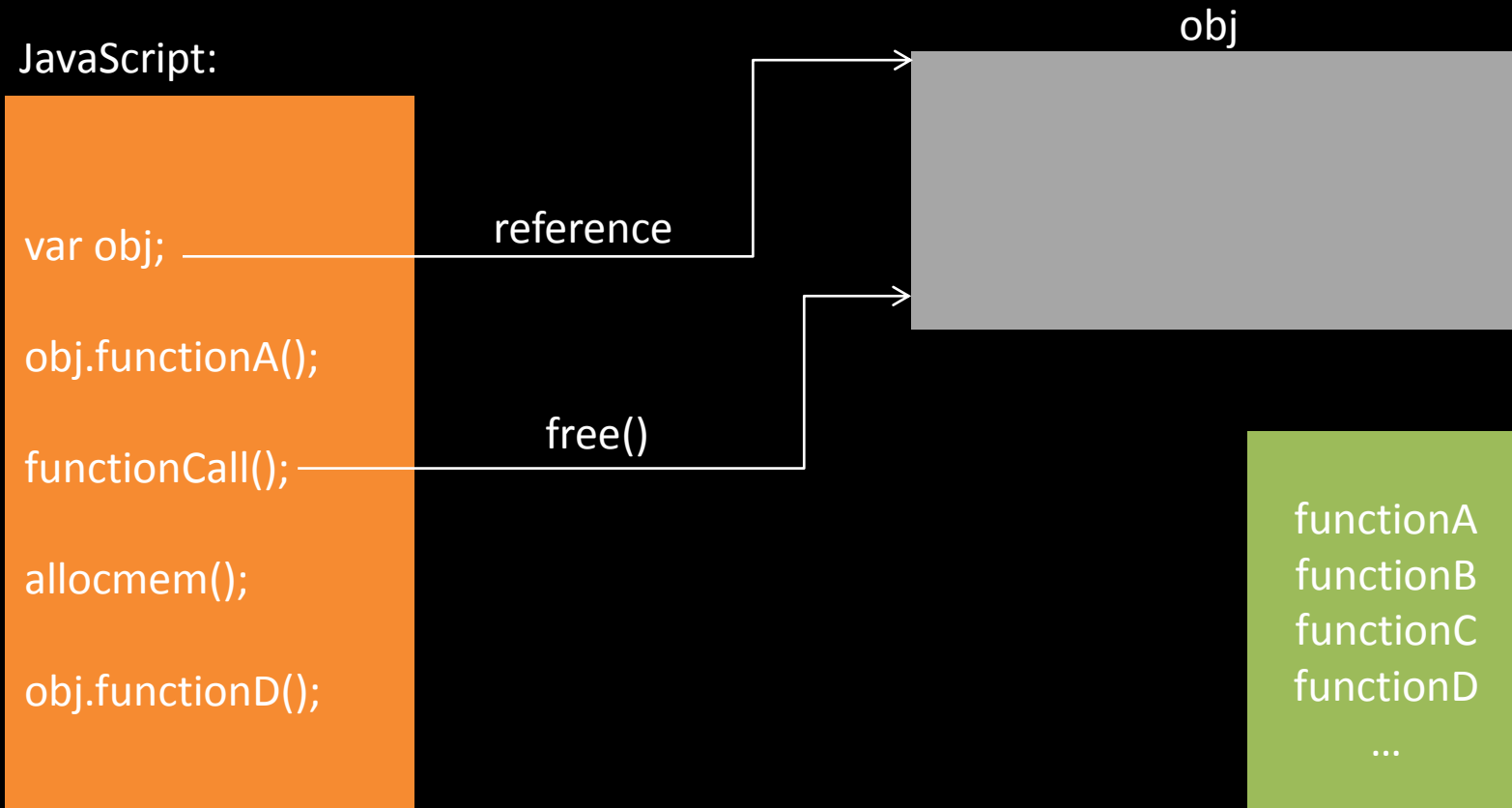
Exploiting a use-after-free vulnerability in WebKit (CVE-2010-1759)



Step 2: Cross-Platform Infection

Phase 3: Remote Exploitation

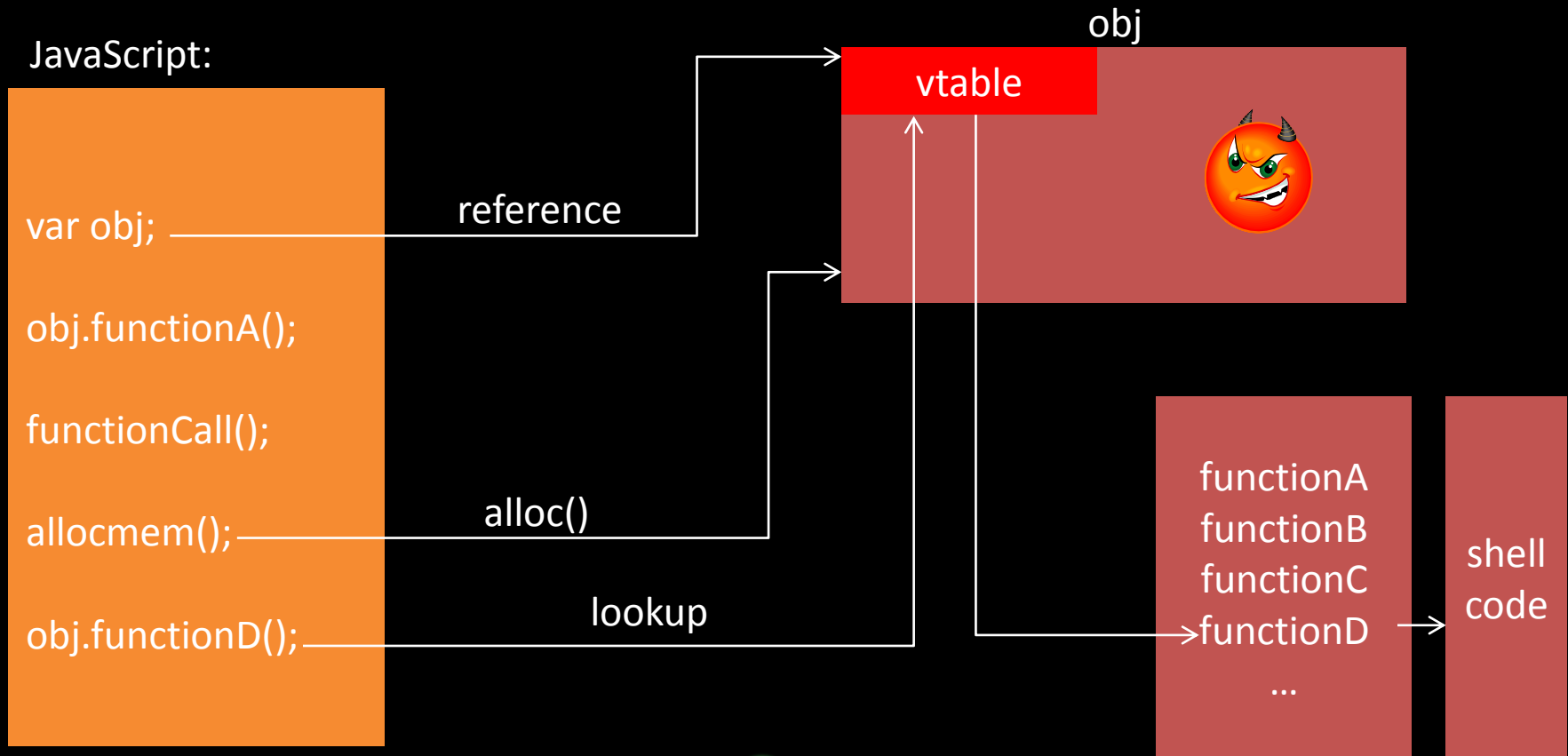
Exploiting a use-after-free vulnerability in WebKit (CVE-2010-1759)



Step 2: Cross-Platform Infection

Phase 3: Remote Exploitation

Exploiting a use-after-free vulnerability in WebKit (CVE-2010-1759)



Step 2: Cross-Platform Infection

Phase 4: Privilege Escalation to Root

Exploiting the vulnerability in volume manager daemon (CVE-2011-1823)
(used also by Gingerbreak [3])

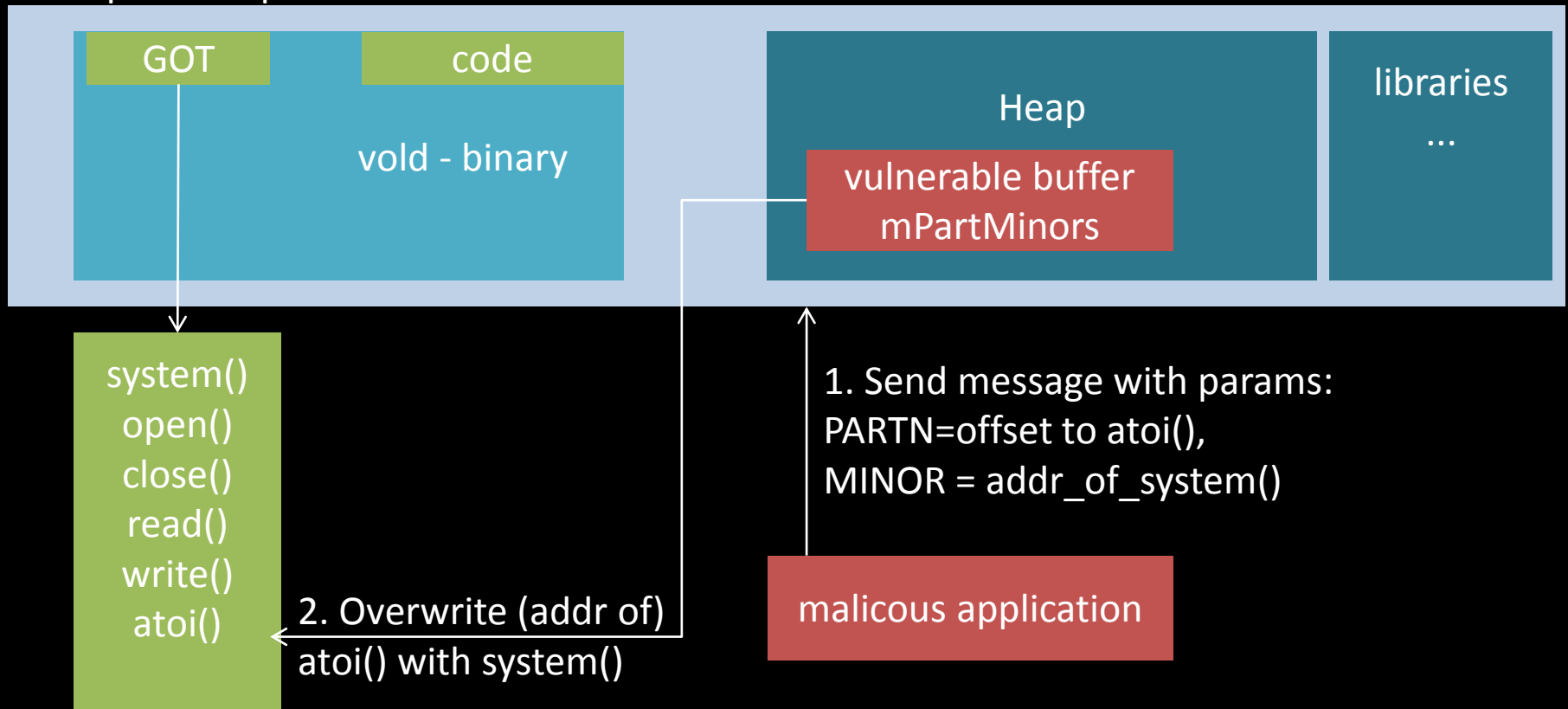


handlePartitionAdded() (system/core/vold/DirectVolume.cpp)

```
int minor = atoi(evt->findParam("MINOR"));
int part_num;
const char *tmp = evt->findParam("PARTN");
if (tmp) {
    part_num = atoi(tmp);
}
[...]
mPartMinors[part_num -1] = minor;
```

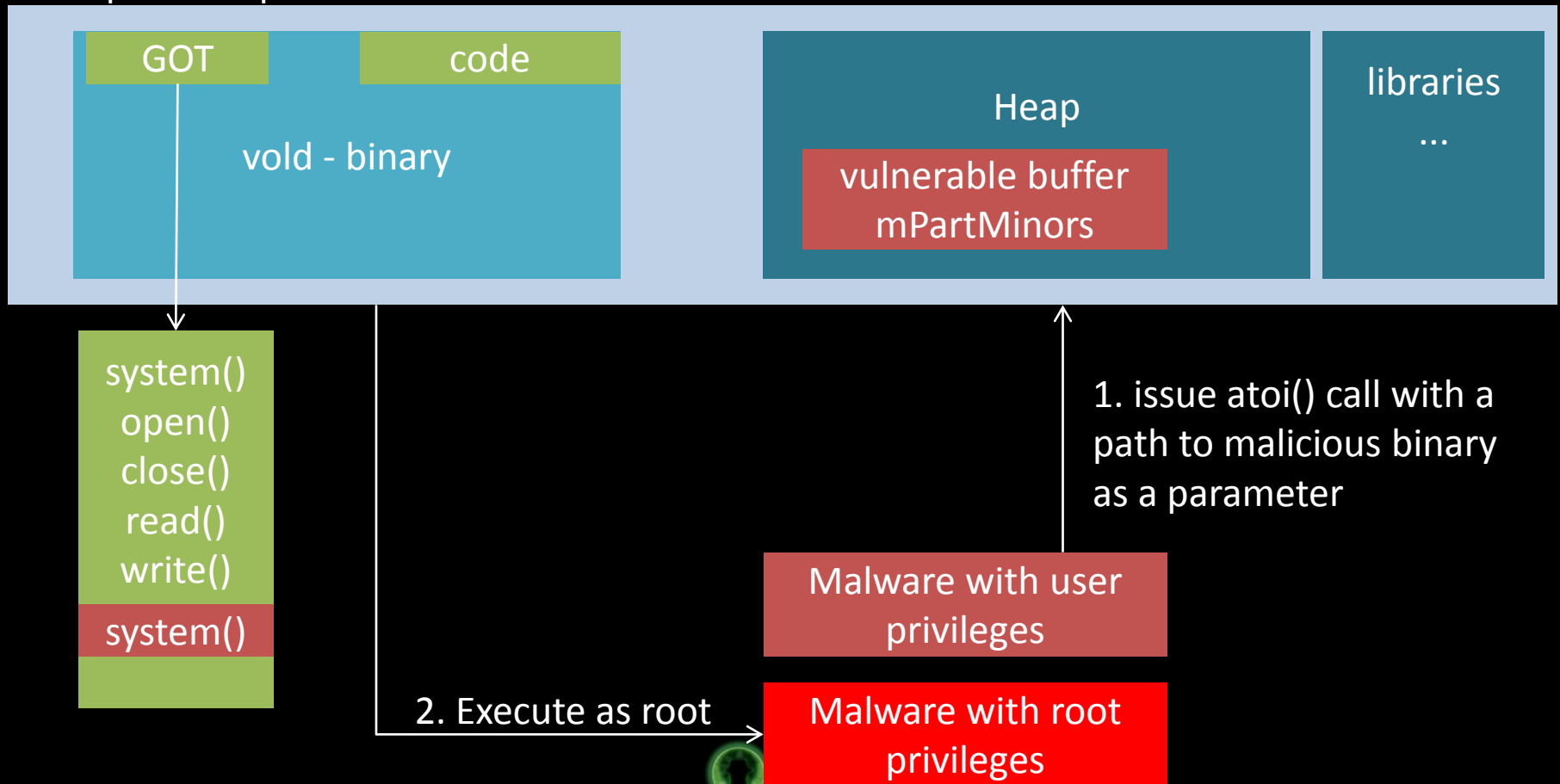
Phase 4: Privilege Escalation to Root (ctd.)

vold process space



Phase 4: Privilege Escalation to Root (ctd.)

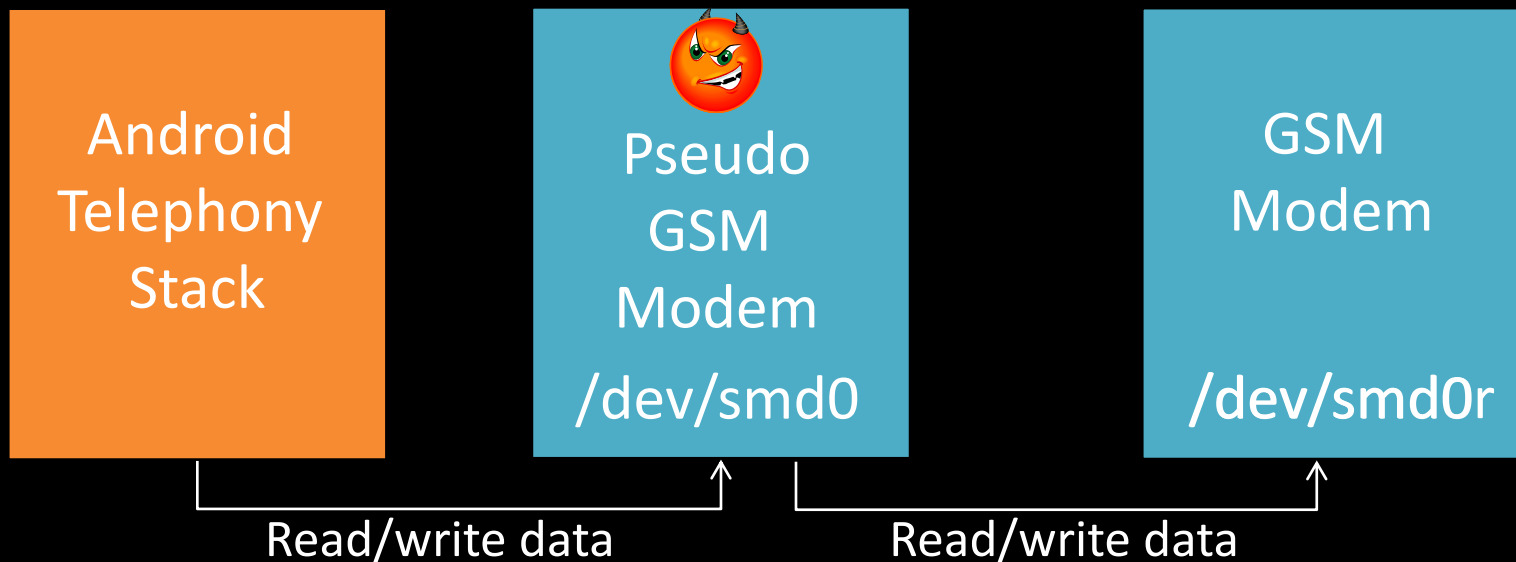
vold process space



Step 4: Stealing mTAN SMS

Man-in-the middle between telephony stack and GSM Modem

- Create pseudo terminal named as GSM Modem
- Rename device associated with GSM Modem



Similar approach was used by for SMS fuzzing by Mulliner and Miller [1]

Step 5: Bypassing Authentication

- Performed manually by the attacker



- Potentially can be automated

Possible Countermeasures: Secure Hardware to Protect Authentication Factors

- Dedicated hardware tokens
 - Less convenient usability (user has to carry an extra device)
- Onboard secure hardware
 - JavaCards, ARM TrustZone, TI MShield, etc.
 - However
 - not available on every mobile phone
 - often controlled and accessible only by specific stakeholders like network operators
 - some have resource limitations

Conclusion and Current Work

- Two-factor authentication schemes with mobile devices fail to capture realistic attacker model
 - They assume trusted mobile device, or at least suppose that one attacker cannot control both, PC and the mobile device
- In contrast to existing online banking malware, the attack via cross-platform infection requires no or little user interaction
- Current work:
 - Other cross-platform infection scenarios (particularly, tethering)
 - Infection in opposite direction (Mobile-to-PC)
 - Targeting other two-factor authentication schemes with mobile phones (photoTAN and signature-based)

References

- [1] C. Mulliner and C. Miller. Injecting SMS messages into smart phones for security analysis. USENIX Workshop on Offensive Technologies, 2009
- [2] A. Stavrou, Z. Wang. Exploiting smart-phone USB connectivity for fun and profit. BlackHat DC 2011
- [3] Root your Gingerbread device with Gingerbreak.
<http://www.xda-developers.com/android/root-your-gingerbread-device-with-gingerbreak/>, 2011
- [4] ICICI Bank. What is SIM-Swap fraud?
<http://www.icicibank.com/online-safe-banking/simswap.html>
- [5] IT-Online, “World-first SMS banking scam exposes weaknesses,”
<http://www.it-online.co.za/2009/07/16/worldfirst-sms-banking-scam-exposes-weaknesses/>, July 2009