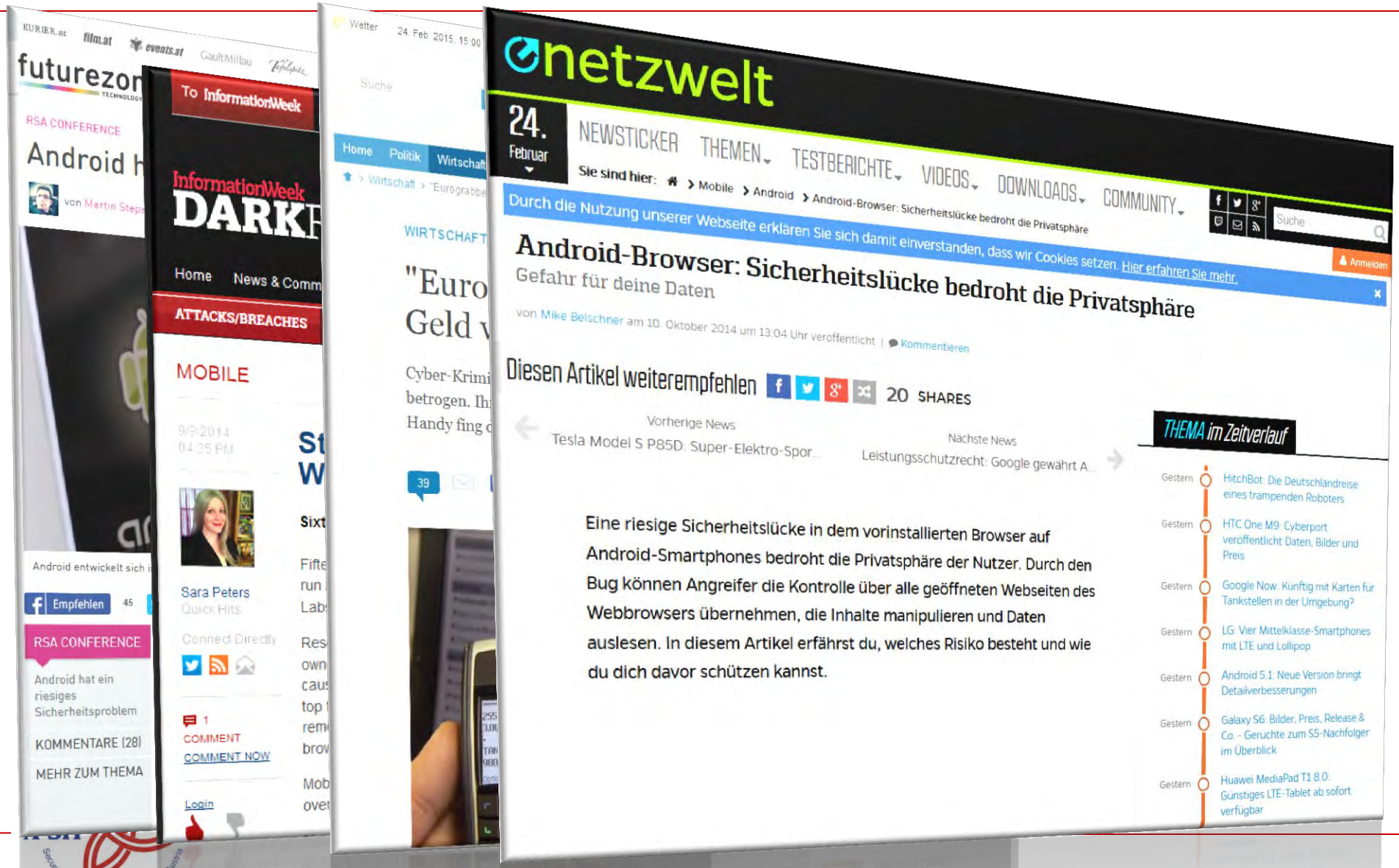
Relevante Sicherheitskriterien aktueller mobiler Plattformen

RTR-Workshop „Sicherheit mobiler Endgeräte“

Thomas Zefferer

Motivation


futurezone
RSA CONFERENCE
Android H
Android entwickelt sich
Empfehlen 45
RSA CONFERENCE
Android hat ein riesiges Sicherheitsproblem
KOMMENTARE (28)
MEHR ZUM THEMA
InformationWeek
DARK
Home
News & Comm
ATTACKS/BREACHES
MOBILE
Sara Peters
Quick Hits
Connect Directly
1 COMMENT
COMMENT NOW
Login
Wetter
24. Feb 2015, 15:00
Home
Politik
Wirtschaft
WIRTSCHAFT
"Euro
Geld
Cyber-Krimi
betrogen. Ih
Handy fing
39
netzwelt
24. Februar
NEWSTICKER
THEMEN
TESTBERICHTE
VIDEOS
DOWNLOADS
COMMUNITY
Sie sind hier: Mobile > Android > Android-Browser: Sicherheitslücke bedroht die Privatsphäre
Durch die Nutzung unserer Webseite erklären Sie sich damit einverstanden, dass wir Cookies setzen. Hier erfahren Sie mehr.
Suche
Anmelden
Android-Browser: Sicherheitslücke bedroht die Privatsphäre
Gefahr für deine Daten
von Mike Belschner am 10. Oktober 2014 um 13:04 Uhr veröffentlicht | Kommentieren
Diesen Artikel weiterempfehlen
20 SHARES
Vorherige News
Tesla Model S P85D: Super-Elektro-Spor...
Nächste News
Leistungsschutzrecht: Google gewährt A...
Eine riesige Sicherheitslücke in dem vorinstallierten Browser auf Android-Smartphones bedroht die Privatsphäre der Nutzer. Durch den Bug können Angreifer die Kontrolle über alle geöffneten Webseiten des Webbrowsers übernehmen, die Inhalte manipulieren und Daten auslesen. In diesem Artikel erfährst du, welches Risiko besteht und wie du dich davor schützen kannst.
THEMA im Zeitverlauf
Gestern HitchBot: Die Deutschlandreise eines trampenden Roboters
Gestern HTC One M9: Cyberport veröffentlicht Daten, Bilder und Preis
Gestern Google Now: Künftig mit Karten für Tankstellen in der Umgebung?
Gestern LG: Vier Mittelklasse-Smartphones mit LTE und Lollipop
Gestern Android 5.1: Neue Version bringt Detailverbesserungen
Gestern Galaxy S6: Bilder, Preis, Release & Co. - Gerüchte zum S5-Nachfolger im Überblick
Gestern Huawei MediaPad T1 8.0: Günstiges LTE-Tablet ab sofort verfügbar

Überblick

- Besonderheiten mobiler Geräte
  - Was können diese Geräte?
  - Wie unterscheiden sie sich von herkömmlichen PCs und Laptops?
- Plattform-Überblick
  - Welche mobile Plattformen gibt es?
  - Wie unterscheiden sie sich?
- Welche Sicherheitsfeatures bieten aktuelle mobile Plattformen?
- Was sind Best Practices bei der Verwendung dieser Features?

Mobile Plattformen

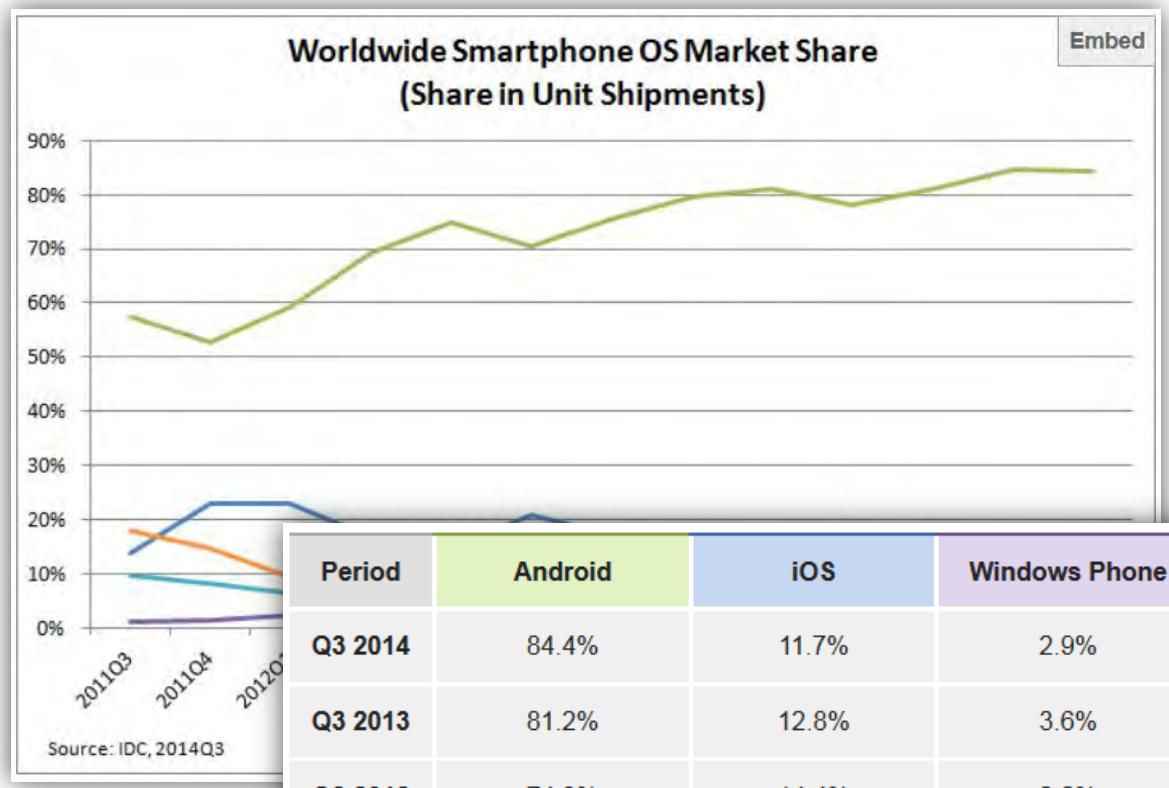
- Kombination unterschiedlicher Aspekte
  - Mobiles Betriebssystem
    - Android
    - iOS
    - Windows Phone
    - BlackBerry
  - Mobiles Endgerät
  - Infrastrukturkomponenten
    - App Stores
    - Update-Mechanismen

- **Gesamtbetrachtung notwendig!**

Herausforderungen mobiler Plattformen

- Mobiler Charakter birgt zusätzliche Gefahren
  - Diebstahl
  - Verlust
- Alternatives Software-Deployment
  - Zentral verwaltete App-Stores
- Besondere Betriebssysteme
  - Sandboxing
  - Permission-Systeme
- Besondere Features
  - GPS, andere Sensoren
- Vermischung von privater und beruflicher Nutzung

Verbreitung



Period	Android	iOS	Windows Phone	BlackBerry OS	Others
Q3 2014	84.4%	11.7%	2.9%	0.5%	0.6%
Q3 2013	81.2%	12.8%	3.6%	1.7%	0.6%
Q3 2012	74.9%	14.4%	2.0%	4.1%	4.5%
Q3 2011	57.4%	13.8%	1.2%	9.6%	18.0%

Quelle: IDC – Analyze the Future
http://www.idc.com/prodserv/smartphone-os-market-share.jsp

Unterschiede zwischen Plattformen

- Unterstützte Sicherheitsfunktionen
  - Permission-Systeme
  - Dateisystem-Verschlüsselung
  - Zugriffskontrolle
- Updates
  - Verfügbarkeit
  - Frequenz
- Technische Möglichkeiten von Apps
  - Zugriff auf Systemfunktionen
  - Verwendung von Hintergrundtasks
- Und vieles mehr…

Zentrale Fragen für EndnutzerInnen

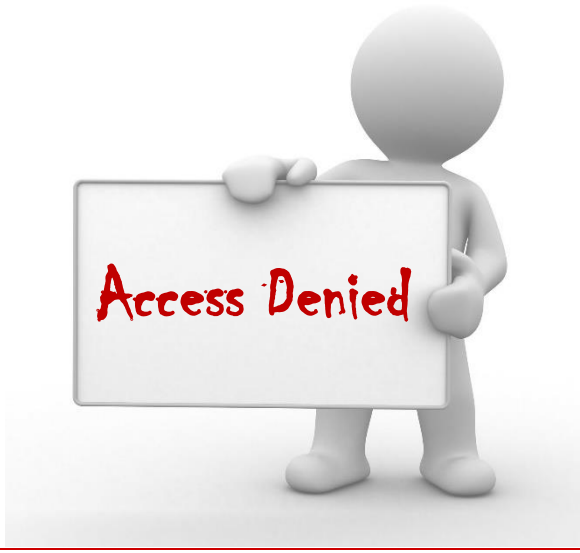
- Welche Sicherheitsfeatures bieten aktuelle Plattformen?
- Worin unterscheiden sich Plattformen?
- Was sind Best Practices bei der Verwendung mobiler Plattformen und derer Sicherheitsfeatures?

Sicherheitsfeatures mobiler Plattformen

- Zugriffskontrolle
- Verschlüsselung
- Permission-Systeme
- Updates
- Software-Deployment

Zugriffskontrolle

- Schutz vor Zugriff über User-Interface
- Verschiedene Ansätze
  - PIN
  - Passwort
  - Fingerabdruck
  - Patterns
  - Face Unlock
  - …
- „First Line of Defense“ bei Diebstahl oder Verlust!
- Relevante Aspekte
  - Entropie
  - Sicherheit und Zuverlässigkeit
  - Benutzerfreundlichkeit



Zugriffskontrolle – PIN/PW – Entropie

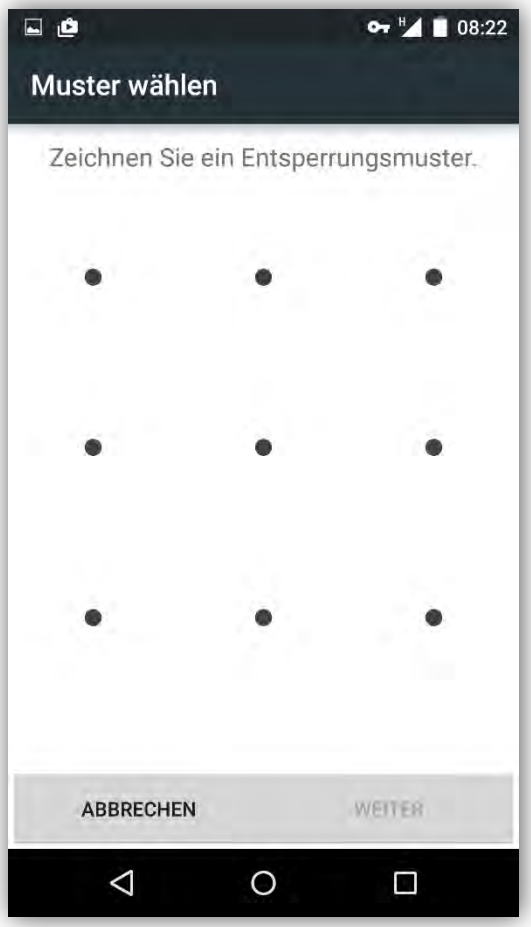
Zumindest alphanumerische Passwörter verwenden!

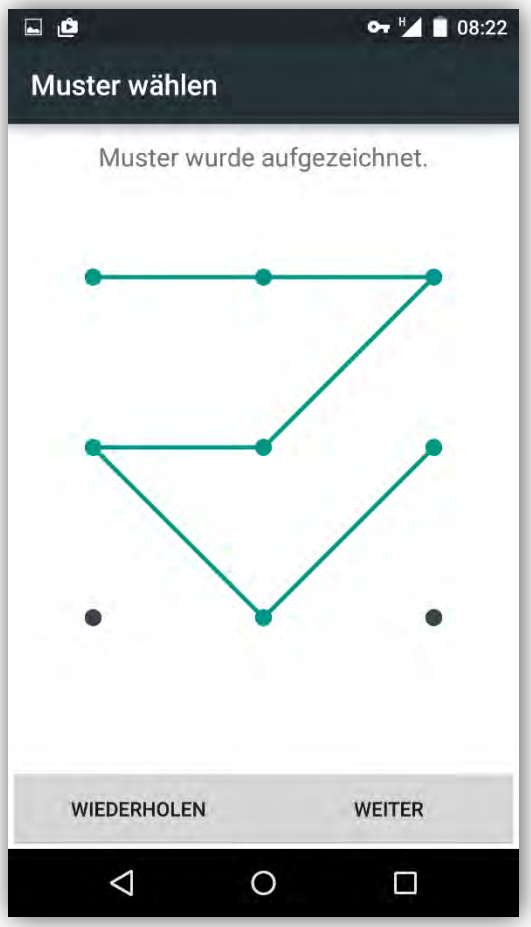
Passwort mit ausreichender Länge wählen!

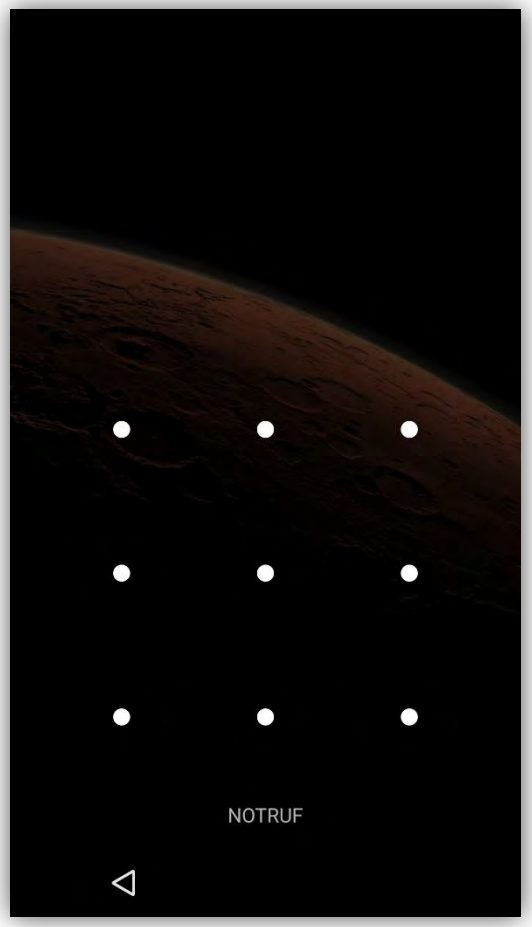
Lock-Screen Type	Length	Chars	Number of passcodes
Numerical	4	10	10000
	6	10	1000000
	8	10	100000000
	10	10	10000000000
Alphanum	4	36	1679616
10/26 letters	6	36	2176782336
	7	36	78364164096
	8	36	2821109907456
	9	36	101559956668416
	10	36	3656158440062980
Alphanum	4	62	14776336
	5	62	916132832
10/52 letters	6	62	56800235584
	7	62	3521614606208
	8	62	218340105584896
	9	62	13537086546263600
Complex	4	107	131079601
	5	107	14025517307
	6	107	1500730351849
	7	107	160578147647843
	8	107	17181861798319200

Quelle: Peter Teufl: Advanced Computer Networks (Vorlesungsunterlagen)
https://sites.google.com/site/acnws2014/

Zugriffskontrolle – Patterns







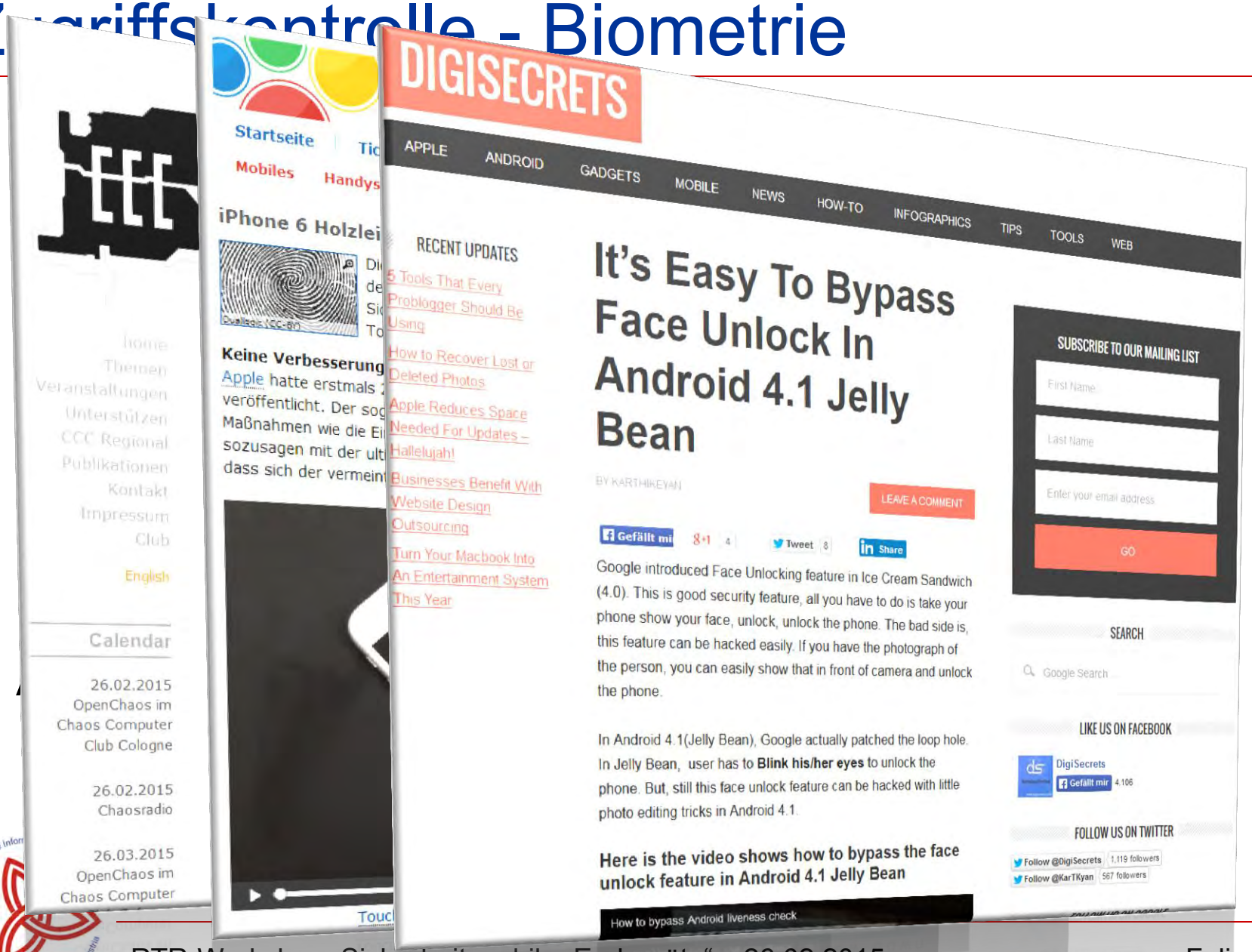
Zugriffskontrolle – Patterns – Entropie

N	# Patterns mit N Punkten	Anzahl PINs mit N Ziffern
2	56	100
3	360	1.000
4	2.280	10.000
5	14.544	100.000
6	92.448	1.000.000
7	588.672	10.000.000
8	3.745.152	100.000.000

Quelle: Peter Teufl: Advanced Computer Networks (Vorlesungsunterlagen)
https://sites.google.com/site/acnws2014/

Zugriffskontrolle - Biometrie

-
-
-
-
-



Verschlüsselung

- PINs/Passwörter/Patterns/etc. schützen nur vor unerlaubtem Zugriff über User-Interface des mobilen Geräts
- Am Gerät gespeicherte Daten bleiben bei Verlust oder Diebstahl des mobilen Geräts trotzdem zugänglich
- Einzige Abhilfe: Verschlüsselung
- Verschlüsselung wird von allen mobilen Plattformen unterstützt
- Jedoch signifikante Unterschiede in Umsetzung

Verschlüsselung – Relevante Aspekte

- Was wird verschlüsselt?
  - Gesamtes Dateisystem
  - Einzelne Dateien
- Welche Verschlüsselungsverfahren werden verwendet?
- Wie wird der verwendete Schlüssel geschützt?
  - Über PIN/Passwort?
  - Über sicheres Hardware-Element?
- Was ist für EndnutzerInnen zu beachten?
  - Verschlüsselung aktivieren!
  - Entsprechend sicheres Passwort verwenden!

Permission-Systeme

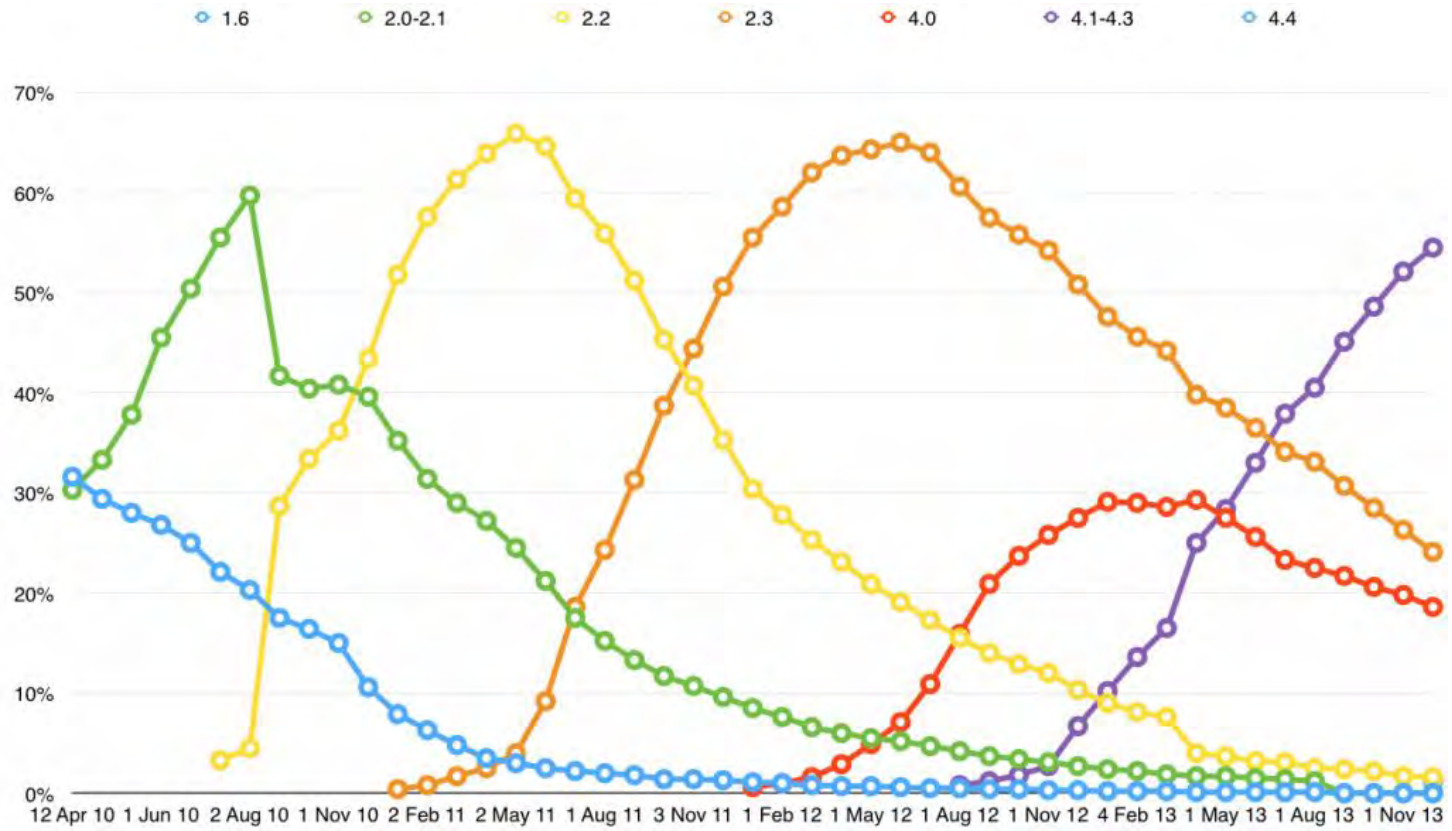
- Regeln Berechtigungen von Apps
- Idee: BenutzerIn bestimmt, was App darf
- Unterschiedliche Ansätze
  - Erteile Permission bei Installation der App (Android)
  - Erteile Permission erst dann wenn sie benötigt wird (iOS)
- Prinzipiell gute Idee, aber Probleme in der Praxis
  - Fehlende Awareness bei BenutzerInnen
  - Benötigte Permissions oft nicht nachvollziehbar
  - Implikationen oft nicht klar

Updates

- Updates sind unumgänglich zum Schließen entdeckter Sicherheitslücken
- Relevante Aspekte
  - Generelle Verfügbarkeit und Frequenz von Updates
  - Reaktionszeit nach Auftreten von Sicherheitslücken
- Hauptproblem: Fragmentierung
  - Betrifft hauptsächlich Android
  - Viele verschiedene Endgeräte und Betriebssystem-Versionen
  - Zahlreiche Modifizierungen durch Gerätehersteller
- Update-Situation speziell unter Android nicht zufriedenstellend

Updates

Verbreitung von Android-Versionen



Quelle: Beyond Devices: Thoughts on Google's Android version charts
http://www.beyonddevic.es/2013/12/30/thoughts-on-googles-android-version-charts/

Software-Deployment

- Wie können Apps durch BenutzerInnen installiert werden?
- Weniger Flexibilität im Vergleich zu Desktop-PCs oder Laptops
- Idee: Zentral verwaltete App-Stores
- Theorie: Über diese App-Stores werden nur geprüfte Apps angeboten
- Praxis: Vor allem unter Android massive Malware-Probleme
  - Malware in offiziellem Google Play Store
  - Offensichtlich keine ausreichenden Überprüfungen
  - Installation von Apps auch über alternative Quellen möglich
- Best Practice
  - Apps nur von vertrauenswürdigen Quellen beziehen!
  - Berechtigungen auf Plausibilität prüfen!
  - Vorsicht speziell unter Android!

Best Practices

- Zugriffsschutz aktivieren und ausreichend sicheren PIN/PW wählen!
- Verschlüsselung aktivieren!
- Angeforderte Permissions auf Plausibilität prüfen!
- Updates einspielen!
- Apps nur von vertrauenswürdigen Quellen beziehen!

Fazit

- Mobile Plattformen bieten viele neue Möglichkeiten – aber bringen auch zahlreiche neue Probleme und Herausforderungen
- Funktionalität vs. Sicherheit vs. Benutzerfreundlichkeit
- Plattformen bieten zahlreiche Features, über die Sicherheit erhöht werden kann
- Basisverständnis von BenutzerInnen notwendig, um Features richtig einzusetzen
- Best Practices bei Verwendung von Sicherheitsfunktionen beachten!

Weiterführende Informationen

- Peter Teufl: Advanced Computer Networks – Vorlesungsunterlagen: https://sites.google.com/site/acnws2014/

- Barrera, David, Paul C. van Oorschot, and Anil Somayaji [2010]. *A Methodology for Empirical Analysis of Permission-Based Security Models and its Application to Android Categories and Subject Descriptors*. In Proceedings of the 17th ACM Conference on Computer and Communications Security, pages 73-84. CCS '10, ACM.
- Bläsing, Thomas, Leonid Batyuk, Aubrey Derrick Schmidt, Seyit Ahmet Camtepe, and Sahin Albayrak [2010]. *An Android Application Sandbox System for Suspicious Software Detection*. In Proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software, Malware 2010, pages 55-62.
- Enck, William and Damien Octeau [2011]. *A Study of Android Application Security*. Proceedings of the 20th USENIX Conference on Security, pages 21-21.
- Teufl, Peter, Thomas Zefferer, and Christof Stromberger [2013a]. *Mobile Device Encryption Systems*. In 28th IFIP TC-11 SEC 2013 International Information Security and Privacy Conference, pages 203-216. Springer.

Vielen Dank!

thomas.zefferer@a-sit.at