Security and Privacy
in Mobile and Web-based Healthcare Interventions/Applications - An overview

James Joshi

Lecture 11

IS 2620

Nov 30, 2017

Paradigm Shift in Technology enabled Healthcare

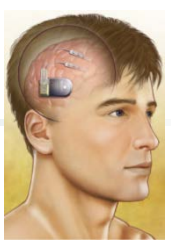
- *Anywhere*, *Anytime* Personalized Healthcare/medicine

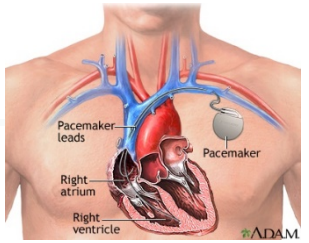
Enablers

- Medical devices, IoT & Sensor technologies
- Mobile and Web technologies,
- Social networking, Cloud computing, Location based services
- Big Data analytics – AI, ML, ...

Many value added features/services

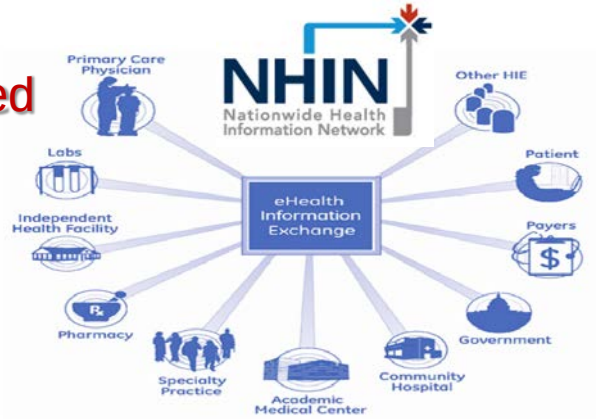
Continuous Monitoring and On-time intervention





in-body/out-body implantable/ wearable devices, sensors

Integrated Care



Social Support

Self-care

mHealth App Spectrum

259K mobile apps in 2016 (up by 57%)

Source:mHealth App developer survey economics 2016

Simple ⟷ *Complex*

Single use mHealth

Focuses on a single purpose for a single user, typically consumer initiated:

- smartphone apps and wearable tech products that support the user to record data which may be communicated to others
- consumer driven, focus on wellness, diet and exercise.

Social mHealth

Draws upon the support and encouragement provided through social networks:

- gamification and competition based apps which encourage users to meet goals
- consumers likely to pursue activities independently.

Integrated mHealth

Links apps and devices with the formal healthcare system:

- mobile technology linking patients and HCPs
- tailored to multiple end users: consumers, physicians and administrators.

Complex mHealth

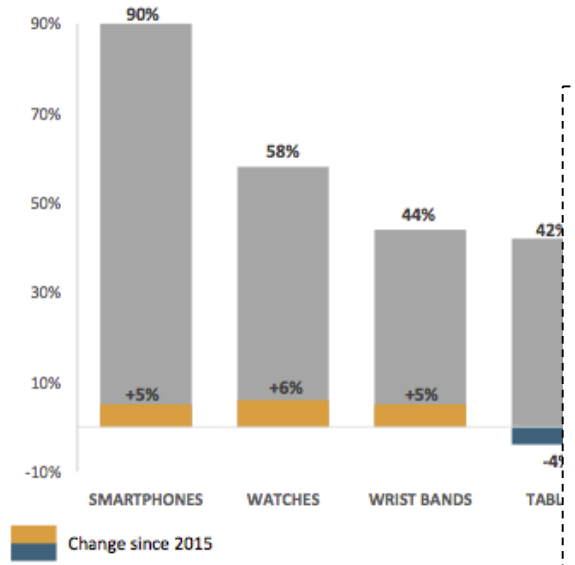
Leverages advanced, integrated analytics for decision support:

- predictive analytics applied to complex data generated through mHealth applications
- focus on achieving optimal management of a specific disease.

Source: Four Dimensions of Effective mHealth, Deloitte US Center for Health Solutions, 2014

SMARTPHONES REMAIN THE MAIN PREFERRED DEVICE FOR MHEALTH APPS

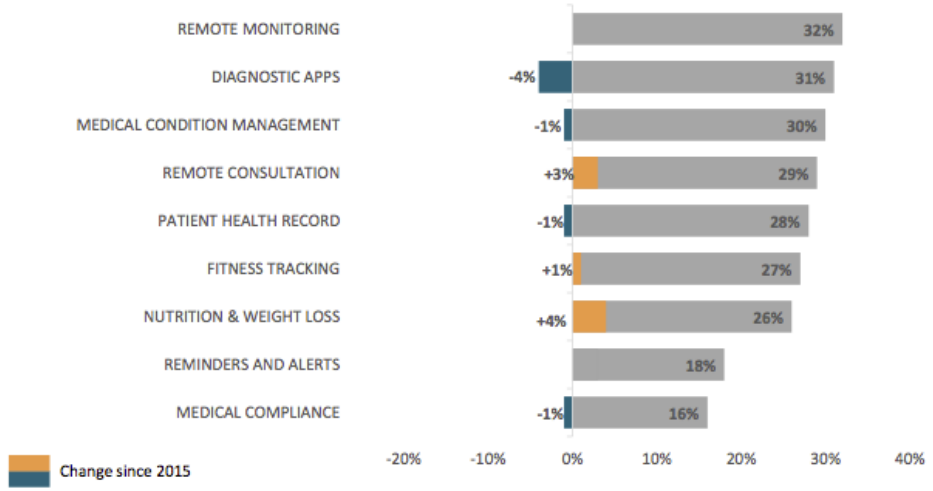
Which devices offer the best market potential for mHealth in the next 5 years?



Source: research2guidance - mHealth App Developer Ecor

REMOTE MONITORING IS NOW THE APP CATEGORY WITH THE GREATEST MARKET POTENTIAL RATING IN THE NEXT 5 YEARS

Which mHealth app categories will offer the highest market potential in the next 5 years?



Source: research2guidance - mHealth App Developer Economics study 2016, n=2600

Source: https://www.pcmag.com/article2/0,2817,2476623,00.asp

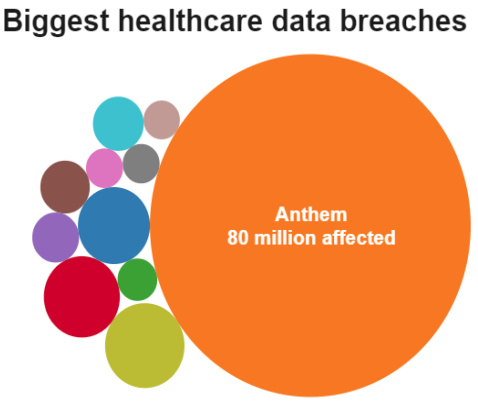
Source:mHealth App developer survey economics 2016

But … Security & Privacy significant concerns

Privacy and Security are the most important concerns

Healthcare is ar vulnerable industr

David Kotz et.al, "Privacy and Security in Mobile Health: A Research Agenda,



"57% of consumer .. report being skeptical of the overall benefits of health information technologies such as patient portals, mobile apps, and electronic health records mainly because of recently reported data hacking and a perceived lack of privacy protection by providers"

"The unwillingness of patients to comprehensively divulge all their medical information rose to 87 percent in the fourth quarter of 2016"

Alarming: Users are concerned " … that their pharmacy prescriptions (90 percent), mental health notes (99 percent) and chronic condition (81 percent) data is being shared beyond their chosen provider and payer to retailers, employers, and or the government without their acknowledgement."
(as per a Black Book survey)

Security and Privacy Issues/Challenges

- At-large

Enablers

- Medical devices, IoT &
- Mobile and Web techno
- Social networking, Clou
  Location based services
- Big Data analytics – AI,

Inherit all their | Leve

Security & Priv
Healthcare

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

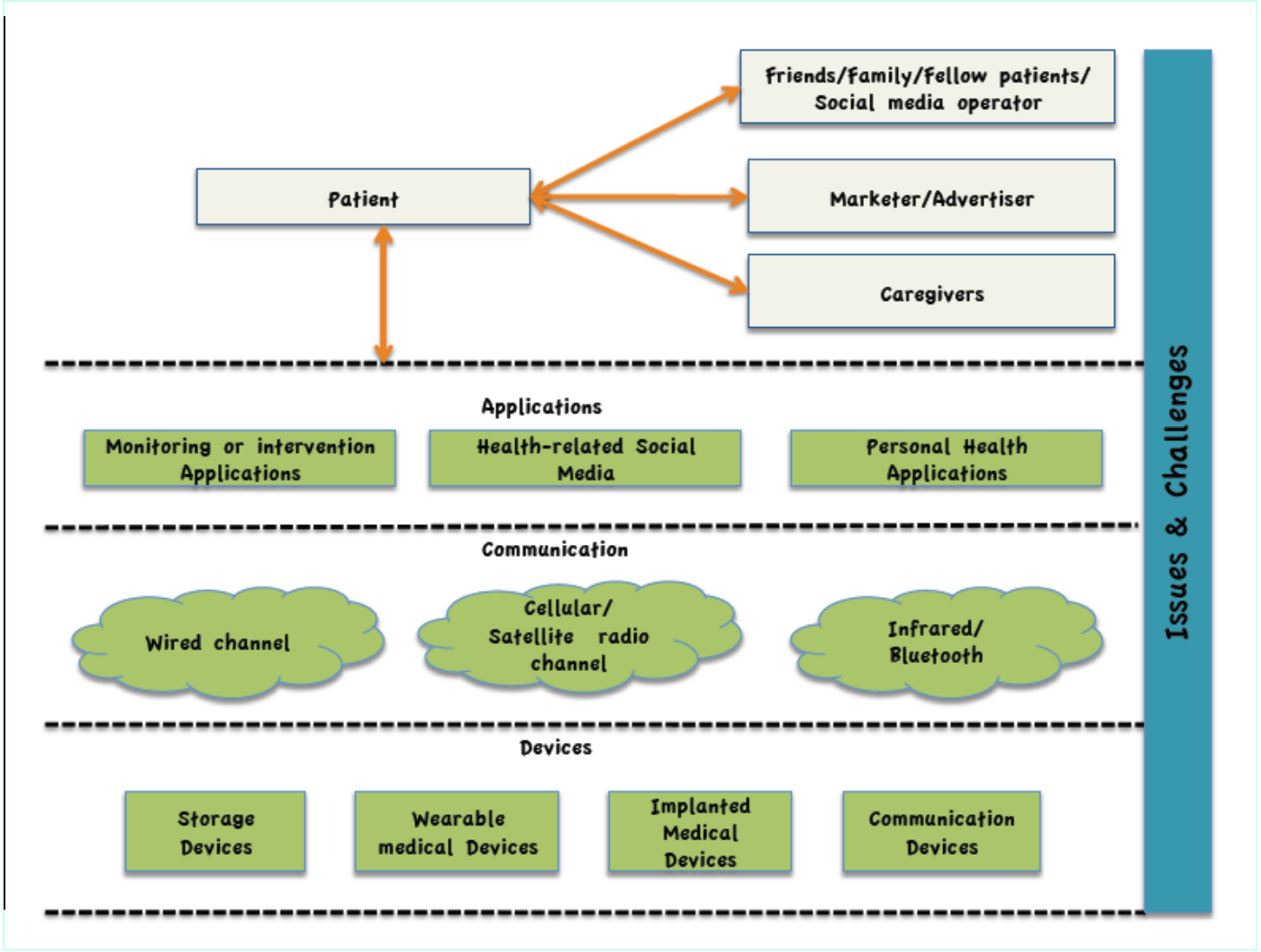
Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities

Source: Healthcare Industry Cybersecurity taskforce June 2017

Security and Privacy Issues/Challenges

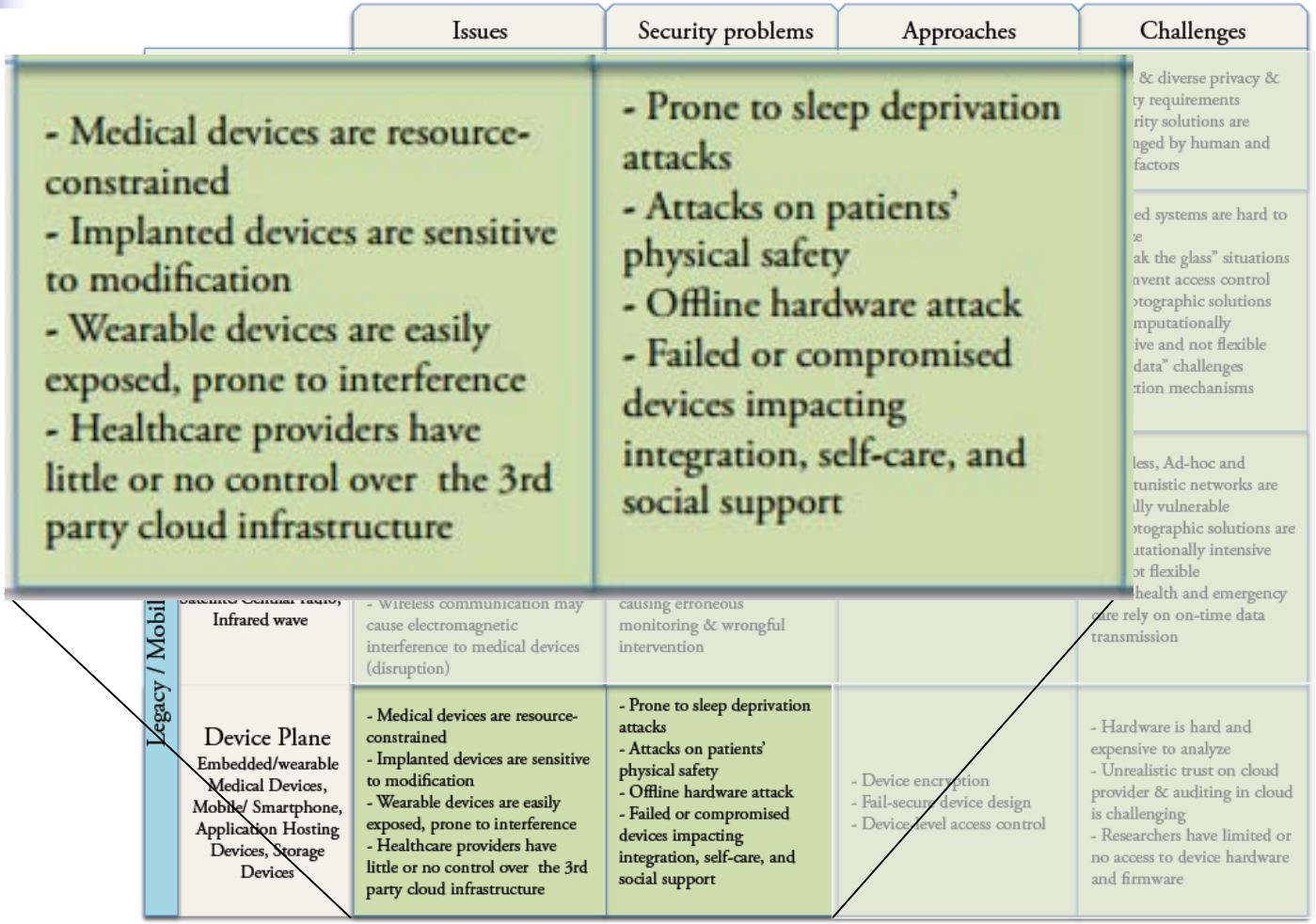
Laws, Regulations, Policies



Security and Privacy Issues/Challenges

		Issues	Security problems	Approaches	Challenges
	User Plane Demographics, Health condition, Physical ability, Mental ability	Demographic profiles and physical & mental abilities of patients are not the same.	- Attacks using non-technical and unintentional vulnerabilities - Targeted attacks on patients with certain characteristics	Human and social factor analysis	- Rich & diverse privacy & security requirements - Security solutions are challenged by human and social factors
Legacy / Mobile / Cloud Infrastructure	**Application Plane** EMR, Tele-Health apps, Personal Health Apps (PHR mgmt, tracking), Health-related social media (OSN, VC)	- Health records are fragmented and dispersed in many facilities - In Tele-Health, a mosaic of applications work with each other, creating a highly collaborative environment - Personal health apps collect extraneous personal info - Quality of information in social media is highly variable	- De-anonymization and inference attacks by linking different data trails - Many possibilities of unauthorized access and identity theft - Social engineering attacks cripple social support systems	- Testing and certification - Design-by-contract - Principle of least privilege - Access control - Data Masking - Cryptographic protocols - Education and training	- Closed systems are hard to analyze - "Break the glass" situations circumvent access control - Cryptographic solutions are computationally intensive and not flexible -"Big data" challenges protection mechanisms
	Communication Plane Wire (copper, coax, fiberoptics, etc.), bluetooth/Zigbee, Satellite/Cellular radio, Infrared wave	- Sensitive patient information is transmitted over public Internet - From monitoring devices to EHR, data travels through multiple vulnerable communication modalities - Wireless communication may cause electromagnetic interference to medical devices (disruption)	- Denial of service impacting monitoring, integrated care, self-care, and social support - Breach of confidentiality of patient info due to tapping or emanation - Loss of data integrity causing erroneous monitoring & wrongful intervention	- Virtual private networks - Intrusion detection - Message authentication - EMI testing	-Wireless, Ad-hoc and opportunistic networks are naturally vulnerable - Cryptographic solutions are computationally intensive and not flexible - Tele-health and emergency care rely on on-time data transmission
	Device Plane Embedded/wearable Medical Devices, Mobile/ Smartphone, Application Hosting Devices, Storage Devices	- Medical devices are resource-constrained - Implanted devices are sensitive to modification - Wearable devices are easily exposed, prone to interference - Healthcare providers have little or no control over the 3rd party cloud infrastructure	- Prone to sleep deprivation attacks - Attacks on patients' physical safety - Offline hardware attack - Failed or compromised devices impacting integration, self-care, and social support	- Device encryption - Fail-secure device design - Device-level access control	- Hardware is hard and expensive to analyze - Unrealistic trust on cloud provider & auditing in cloud is challenging - Researchers have limited or no access to device hardware and firmware

Security and Privacy Issues/Challenges



Security and Privacy Issues/Challenges

- Sensitive patient information is transmitted over public Internet
- From monitoring devices to EHR, data travels through multiple vulnerable communication modalities
- Wireless communication may cause electromagnetic interference to medical devices (disruption)

- Denial of service impacting monitoring, integrated care, self-care, and social support
- Breach of confidentiality of patient info due to tapping or emanation
- Loss of data integrity causing erroneous monitoring & wrongful intervention

Legacy / Mobile /Cl	fiberoptics, etc.), bluetooth/Zigbee, Satellite/Cellular radio, Infrared wave	multiple vulnerable communication modalities - Wireless communication may cause electromagnetic interference to medical devices (disruption)	or emanation - Loss of data integrity causing erroneous monitoring & wrongful intervention	- Message authentication - EMI testing	computationally intensive and not flexible - Tele-health and emergency care rely on on-time data transmission
	Device Plane Embedded/wearable Medical Devices, Mobile/ Smartphone, Application Hosting Devices, Storage Devices	- Medical devices are resource-constrained - Implanted devices are sensitive to modification - Wearable devices are easily exposed, prone to interference - Healthcare providers have little or no control over the 3rd party cloud infrastructure	- Prone to sleep deprivation attacks - Attacks on patients' physical safety - Offline hardware attack - Failed or compromised devices impacting integration, self-care, and social support	- Device encryption - Fail-secure device design - Device-level access control	- Hardware is hard and expensive to analyze - Unrealistic trust on cloud provider & auditing in cloud is challenging - Researchers have limited or no access to device hardware and firmware

S&P Challenges

- Data sharing and consent management
- Access control and authentication
  - Loss, theft can result: in data privacy and inaccuracy issues
- Privacy and Anonymity
  - Anonymization, Behavioral privacy, Inference, etc.
  - Third-party connection
- User plane issues
  - Demographic, health conditions – usability, health situations
  - Education, training and awareness
- Policies and Compliance
  - Multiple stakeholders – personal, hospital, …
    - "Covered entities"?
    - Wellness apps are outside HIPAA, but integrate with EHR?
  - Need to make sure policies/standards are followed
    - Cloud & hospital; gov and device manufacturers/apps, etc.

Social Engg attacks
Phishing scams

Need to emphasize *Secure-by-Design, Risk-based approaches*

BigData & Security and Privacy Threats

"Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"

Alan Westin, Privacy and Freedom, 1967

What does it mean to achieve privacy?

FTC Fair Information Protection Principles
- Notice/Awareness
- Choice/Consent
- Access/Participation
- Integrity/Security
- Enforcement/Redress

OECD Privacy Principles
- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness principle
- Individual participation
- Accountability

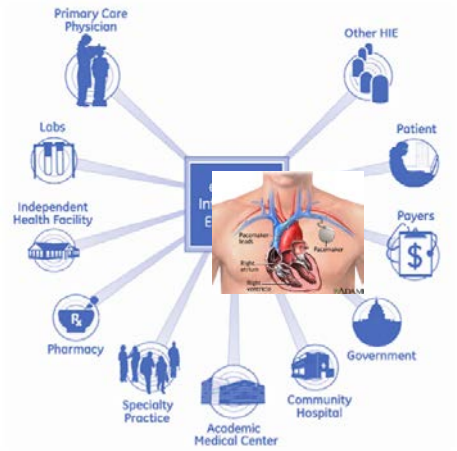
EU guidelines
- ...
-Fairness principle
-Limitation principle
-Right to be forgotten
-Data portability
. ..

HIPAA
COPPA
...

Big Data makes it increasingly difficult to enforce these principles / requirements !!

BigData & Security and Privacy Threats

- Newer data mining, machine learning/ AI tools can unearth/infer sensitive information
  - Consent to new info may not be possible (inference) !!
  - Notice is not really there
  - Data quality/accuracy is not guaranteed
    - Possible false diagnosis, wrong treatment, etc.
  - ...



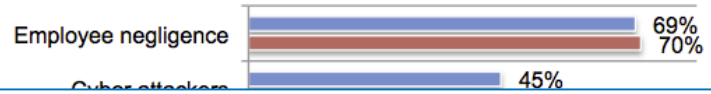
Security and Privacy Issues/Challenges

Threat agents:

Insider OR *Outsider*

Malicious or Inadv

Figure 5. Security threats healthcare organizations worry about most
Three responses permitted



Attack sources by industry

1 January 2016 through 31 December 2016

	Industry sector	% Malicious insider	% Inadvertent actor	% Outsiders
1	Financial services	5%	53%	42%
2	Information and communications	1%	3%	96%
3	Manufacturing	4%	5%	91%
4	Retail	2%	7%	91%
5	Healthcare	25%	46%	29%

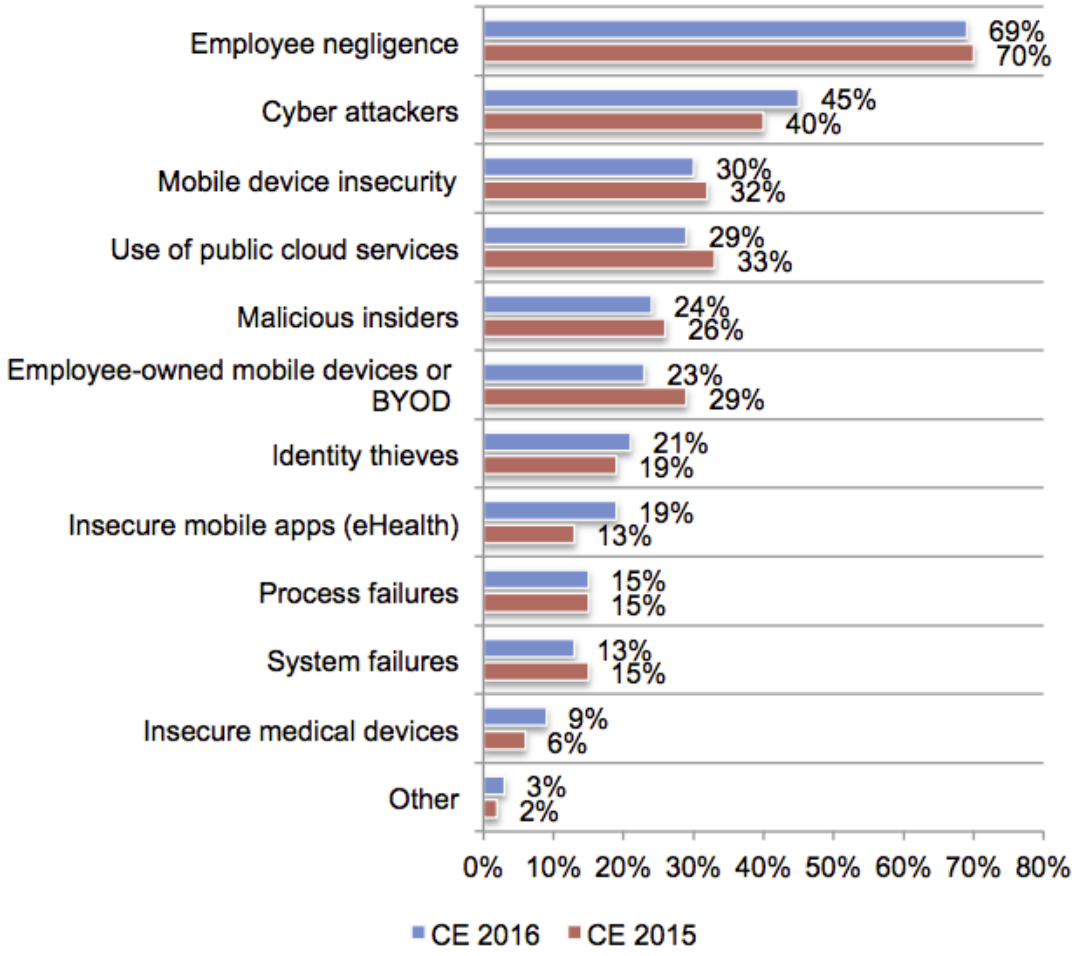
Fewer

More

Figure 9: Attack sources by industry – 1 January 2016 through 31 December 2016.

Case study

Figure 5. Security threats healthcare organizations worry about most
Three responses permitted



Some new approaches

- Privacy aware, context /semantic based / Attribute based AC
  - Secure data fusion
  - Semantic heterogeneity, multiple policies – integration/combination;
  - Content, Concept based access
  - Trust, Risk aware
  - Insider Threat aware
    - Machine learning to capture cybersecurity indicators
      - Health context
      - Insider threats

Some new approaches

Cryptographic approaches include

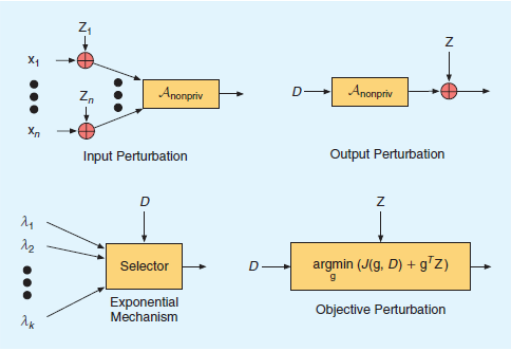
- Attribute based encryption for access control
  - User privacy / protection of policies
- Searchable encryption
- Privacy preserving computation
- Privacy preserving data mining and Machine learning
- Blockchain & hashgraph

Some new approaches

- Anonymization
  - K-anonymity and extensions
  - Structural preserving anonymization
  - (not composable)
- Differential privacy
  - (composable)
- Privacy preserving Data Mining and Machine learning
- ----

Important anonymization features for Big Data

- Controlled Linkability (for fusion)
- Composability
- Anonymization of dynamic/stream data
- Computability for large data volumes
- Decentralized anonymization



Some of our efforts: Intimate Partner Violence (IPV)

30% of women impacted globally (as per WHO, CDC)

Collaboration with:

- Rose Constantino (School of Nursing)
- Balaji Palanisamy (SCI)

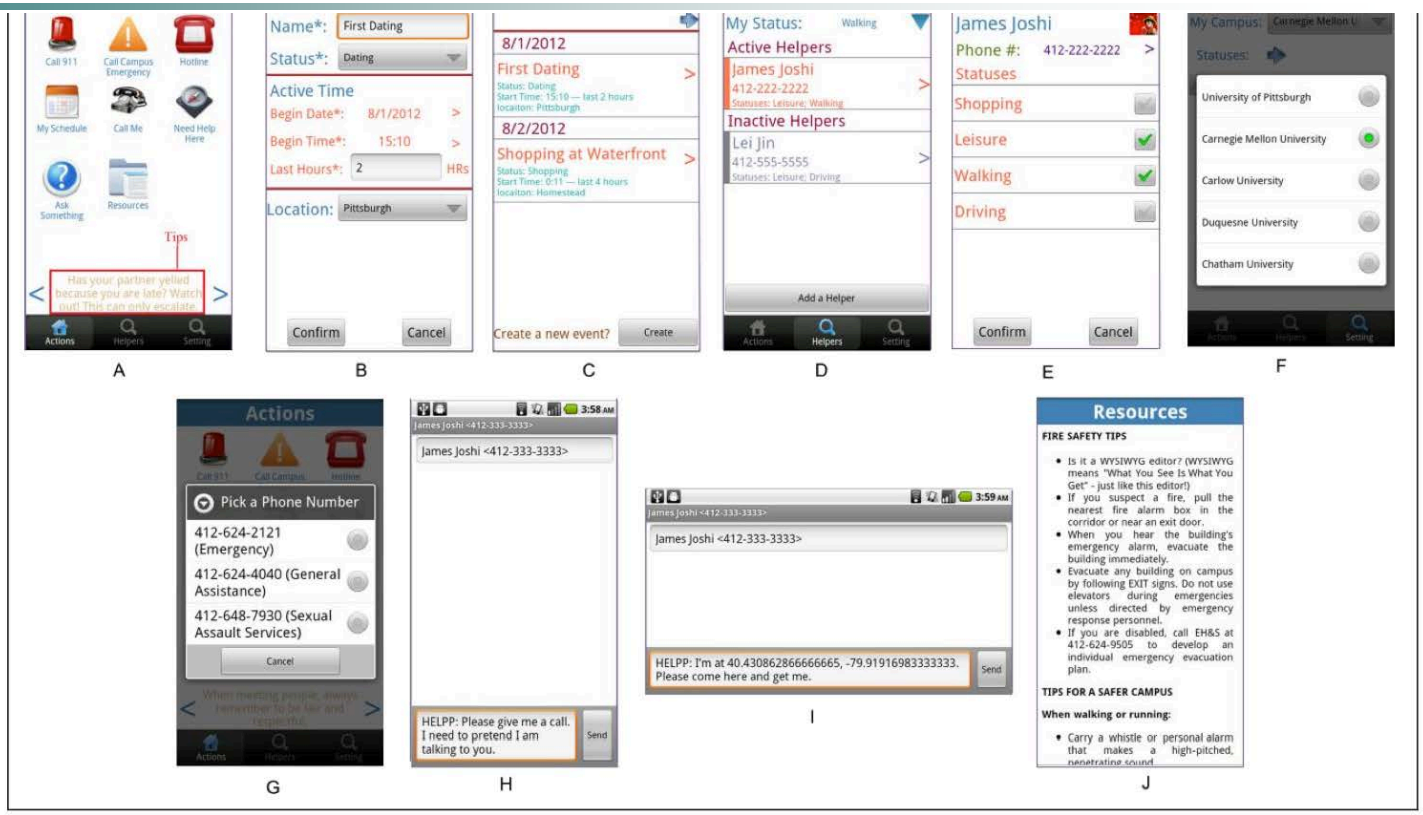
HELPP Zone

(Health, Education on safety, Legal Participant Preferred)

Just-in-time communication and intervention from and by trusted contacts

Text based messasing

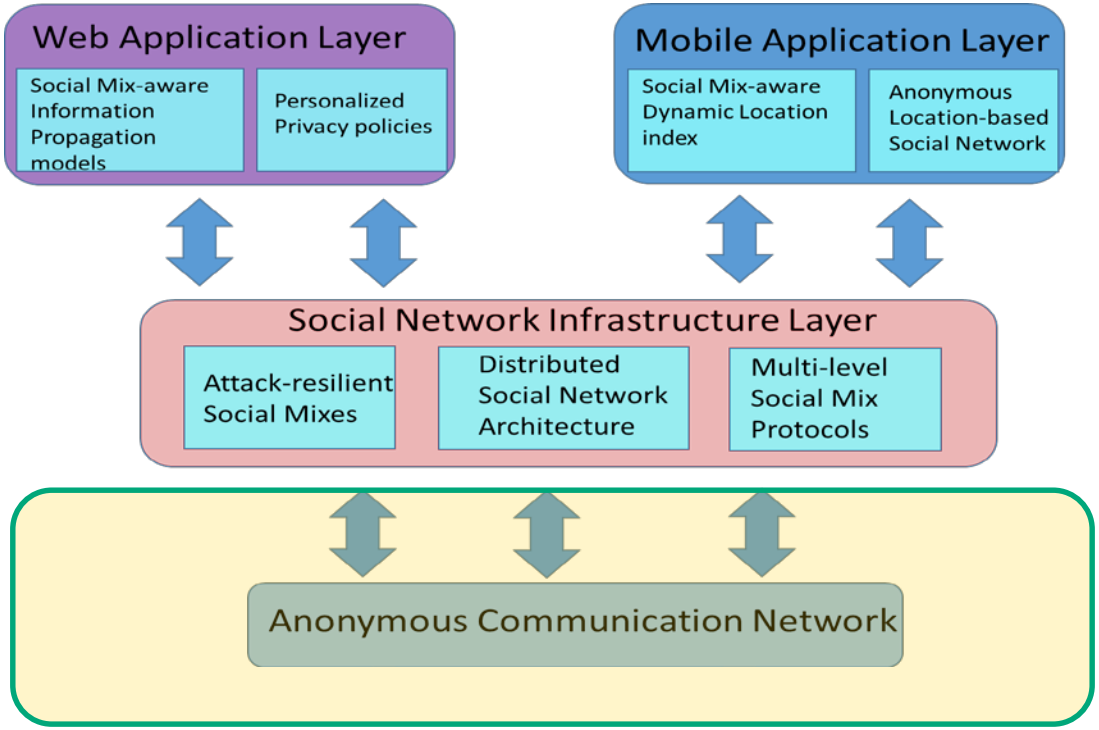
Dynamic trusted contacts



Rose Constantino, Amirreza Masoumzadeh, Lei Jin, James Joshi, Joseph Burroughs, Dominique de la Cruz, “HELPP Zone App and TMI: Disrupting Intimate Partner Violence in College Students” 2013 International Nursing High-end Forum (INHF), China, 22nd - 23rd June, 2013.

A. Masoumzadeh, L. Jin, J. Joshi, and R. Constantino, "HELPP Zone: Towards Protecting College Students from Dating Violence," in iConference 2013 Proceedings, 2013, pp. 925-928.

LEAF System:
(Lending Encouragement, Affirming Futures)



Web app
Social Network
Mobile app

LEAF:A Privacy-conscious Social Network-based Intervention Tool for IPV Survivors

Balaji Palanisamy Sheldon Sensenig James Joshi Rose Constantino†
School of Information Sciences, University of Pittsburgh †*School of Nursing, University of Pittsburgh*

LEAF Social Network

(a) An example LEAF netw

Privacy and Anonymity

Protecting Source Privacy
sender's identity cannot be inferred

Protecting Participant Privacy
willingness to participate increases when anonymity is guaranteed

Protecting Recipient Privacy
Recipient may wish to forward a message from another user to his friends remain anonymous

Protecting Location Privacy
Users should be able to use location-aware resources without revealing their location

Social Mix Mechanism

ymous communication

Conclusions

- Huge potential for *anytime, anywhere*, personalized medicine/healthcare
  - Many value added services/features
- Security and privacy challenges are significant and need to be addressed
  - Insider threat is a significant component.

Thanks !!

Readings

- Rose Constantino, Amirreza Masoumzadeh, Lei Jin, James Joshi, Joseph Burroughs, Dominique de la Cruz, “HELPP Zone App and TMI: Disrupting Intimate Partner Violence in College Students” 2013 International Nursing High-end Forum (INHF), China, 22nd - 23rd June, 2013.

  A. Masoumzadeh, L. Jin, J. Joshi, and R. Constantino, "HELPP Zone: Towards Protecting College Students from Dating Violence," in iConference 2013 Proceedings, 2013, pp. 925-928.

4. Is privacy preserving machine learning realistic?

- Ongoing efforts ...
  - Differentially private machine learning
    - Managing noise vs privacy budget
      - Scale of noise is inversely related to privacy budget
    - Global sensitivity issues
    - Learning Private data release
      - used for machine learning or based on machine learning algorithm
  - Machine learning over encrypted data
    - Binary classification algorithms [Graepel et al., 2012]
    - Extremely Random Forest & naïve Byes : learning and prediction [Aslett et al. , 2015)]
    - Two party computation framework [Bost et al., 2014]
      - Tailored approximation to statistical machine learning models
  - Privacy preserving deep learning [Shokri et al. 2015, Abadi et al. 2016]

May not be practical for atleast sometime

Epilepsy attacks
Phishing

Capture device id, location, demographic

		Issues	Security problems	Approaches	Challenges
	User Plane Demographics, Health condition, Physical ability, Mental ability	Demographic profiles and physical & mental abilities of patients are not the same.	- Attacks using non-technical and unintentional vulnerabilities - Targeted attacks on patients with certain characteristics	Human and social factor analysis	- Rich & diverse privacy & security requirements - Security solutions are challenged by human and social factors
Legacy / Mobile / Cloud Infrastructure	**Application Plane** EMR, Tele-Health apps, Personal Health Apps (PHR mgmt, tracking), Health-related social media (OSN, VC)	- Health records are fragmented and dispersed in many facilities - In Tele-Health, a mosaic of applications work with each other, creating a highly collaborative environment - Personal health apps collect extraneous personal info - Quality of information in social media is highly variable	- De-anonymization and inference attacks by linking different data trails - Many possibilities of unauthorized access and identity theft - Social engineering attacks cripple social support systems	- Testing and certification - Design-by-contract - Principle of least privilege - Access control - Data Masking - Cryptographic protocols - Education and training	- Closed systems are hard to analyze - "Break the glass" situations circumvent access control - Cryptographic solutions are computationally intensive and not flexible -"Big data" challenges protection mechanisms
	Communication Plane Wire (copper, coax, fiberoptics, etc.), bluetooth/Zigbee, Satellite/Cellular radio, Infrared wave	- Sensitive patient information is transmitted over public Internet - From monitoring devices to EHR, data travels through multiple vulnerable communication modalities - Wireless communication may cause electromagnetic interference to medical devices (disruption)	- Denial of service impacting monitoring, integrated care, self-care, and social support - Breach of confidentiality of patient info due to tapping or emanation - Loss of data integrity causing erroneous monitoring & wrongful intervention	- Virtual private networks - Intrusion detection - Message authentication - EMI testing	-Wireless, Ad-hoc and opportunistic networks are naturally vulnerable - Cryptographic solutions are computationally intensive and not flexible - Tele-health and emergency care rely on on-time data transmission
	Device Plane Embedded/wearable Medical Devices, Mobile/ Smartphone, Application Hosting Devices, Storage Devices	- Medical devices are resource-constrained - Implanted devices are sensitive to modification - Wearable devices are easily exposed, prone to interference - Healthcare providers have little or no control over the 3rd party cloud infrastructure	- Prone to sleep deprivation attacks - Attacks on patients' physical safety - Offline hardware attack - Failed or compromised devices impacting integration, self-care, and social support	- Device encryption - Fail-secure device design - Device-level access control	- Hardware is hard and expensive to analyze - Unrealistic trust on cloud provider & auditing in cloud is challenging - Researchers have limited or no access to device hardware and firmware

Issues	Security problems	Approaches	Challenges
- Health records are fragmented and dispersed in many facilities - In Tele-Health, a mosaic of applications work with each other, creating a highly collaborative environment - Personal health apps collect extraneous personal info - Quality of information in social media is highly variable	- De-anonymization and inference attacks by linking different data trails - Many possibilities of unauthorized access and identity theft - Social engineering attacks cripple social support systems	- Testing and certification - Design-by-contract - Principle of least privilege - Access control - Data Masking - Cryptographic protocols - Education and training	- Closed systems are hard to analyze - "Break the glass" situations circumvent access control - Cryptographic solutions are computationally intensive and not flexible -"Big data" challenges protection mechanisms
- Sensitive patient information is transmitted over public Internet - From monitoring devices to	- Denial of service impacting monitoring, integrated care, self-care, and social support - Breach of confidentiality of	- Virtual private networks	-Wireless, Ad-hoc and opportunistic networks are naturally vulnerable - Cryptographic solutions are
- Medical devices are resource-constrained - Implanted devices are sensitive to modification - Wearable devices are easily exposed, prone to interference - Healthcare providers have little or no control over the 3rd party cloud infrastructure	- Prone to sleep deprivation attacks - Attacks on patients' physical safety - Offline hardware attack - Failed or compromised devices impacting integration, self-care, and social support	- Device encryption - Fail-secure device design - Device-level access control	- Hardware is hard and expensive to analyze - Unrealistic trust on cloud provider & auditing in cloud is challenging - Researchers have limited or no access to device hardware and firmware